



System Administration Guide for Cisco Unity Connection

Release 7.x
Revised May 2010

Americas Headquarters

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

Text Part Number: OL-17017-01

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

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

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

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

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

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

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

System Administration Guide for Cisco Unity Connection Release 7.x
© 2008 – 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xix**

- Audience and Use **xix**
- Documentation Conventions **xix**
- Cisco Unity Connection Documentation **xx**
- Obtaining Documentation and Submitting a Service Request **xx**
- Cisco Product Security Overview **xx**

CHAPTER 1

Configuring the Browser on an Administrator Workstation **1-1**

- Firefox **1-1**
- Microsoft Internet Explorer **1-2**

CHAPTER 2

Accessing and Using Cisco Unity Connection Administration **2-1**

- Accessing and Exiting Cisco Unity Connection Administration **2-1**
- Cisco Unity Connection Administration User Interface **2-2**
- Using Cisco Unity Connection Administration Help **2-2**
- Finding Records in Cisco Unity Connection Administration **2-3**

CHAPTER 3

Administrative Tools **3-1**

- Application Plug-ins **3-1**
- Cisco Object Backup and Restore Application Suite (COBRAS) **3-2**
- Cisco Unity Connection Administration **3-2**
- Cisco Unity Connection Bulk Administration Tool **3-2**
- Cisco Unity Connection Bulk Edit Utility **3-3**
- Cisco Unity Connection Custom Keypad Mapping Tool **3-4**
- Cisco Unity Connection Grammar Statistics Tool **3-4**
- Cisco Unity Connection Import and Synch Users Tools **3-4**
- Cisco Unity Connection Migrate Messages Utility **3-5**
- Cisco Unity Connection Migrate Users Utility **3-6**
- Cisco Unity Connection Serviceability **3-6**
- Cisco Unity Connection Task Management Tool **3-7**
- Disaster Recovery System **3-7**
- Cisco Voice Technology Group Subscription Tool **3-7**

Real-Time Monitoring Tool	3-7
Cisco Unified Serviceability	3-8
Remote Database Administration Tools	3-8
Enabling Database Access for Remote Administration Tools	3-9
Cisco Utilities Database Link for Informix (CUDLI)	3-10
Connection User Data Dump (CUDD)	3-10
Wallet Card Wizard	3-10

CHAPTER 4

Call Management Overview	4-1
Overview of Call Management Concepts	4-1
Call Handlers	4-2
Directory Handlers	4-2
Interview Handlers	4-3
Call Routing Tables	4-3
How Call Routing Rules Work	4-4
Using Routing Rules with the Route from Next Call Routing Rule Action	4-5
Restriction Tables	4-6
How Restriction Tables Work	4-6
Schedules and Holidays	4-8
Default Cisco Unity Connection Automated Attendant Behavior	4-9

CHAPTER 5

Creating a Call Management Plan	5-1
Creating a Call Management Map	5-1
Implementing a Call Management Plan	5-2

CHAPTER 6

Managing Call Handlers	6-1
Overview: Default Call Handlers	6-1
Creating, Modifying, and Deleting Call Handler Templates	6-2
Creating Call Handlers	6-4
Modifying Call Handlers	6-4
Overview of Call Handler Greetings	6-6
Managing Call Handler Greetings	6-7
Managing Caller Input During Greetings	6-8
Offering One-Key Dialing During Call Handler Greetings	6-8
Offering System Transfers	6-9
Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter	6-10
Changing Phone Language Settings	6-11

Taking Messages	6-11
Transferring Calls	6-12
Deleting Call Handlers	6-12

CHAPTER 7

Managing Directory Handlers	7-1
Overview: Default Directory Handler	7-1
Creating a Directory Handler	7-1
Modifying a Directory Handler	7-2
Changing Phone Language Settings	7-3
Routing Calls to a Voice Directory Handler	7-3
Deleting a Directory Handler	7-4

CHAPTER 8

Managing Interview Handlers	8-1
Creating Interview Handlers	8-1
Modifying Interview Handlers	8-2
Changing Phone Language Settings	8-2
Deleting Interview Handlers	8-3

CHAPTER 9

Managing Call Routing Tables	9-1
Overview: Default Call Routing Rules	9-1
Adding Call Routing Rules	9-2
Modifying Call Routing Rules	9-2
Changing Phone Language Settings	9-2
Changing the Order of Call Routing Rules	9-3
Deleting Call Routing Rules	9-3

CHAPTER 10

Managing Schedules and Holidays	10-1
Overview: Default Schedules	10-1
Designating Holidays	10-1
Creating Schedules	10-2
Modifying Schedules	10-2
Deleting Schedules	10-3

CHAPTER 11

Managing Restriction Tables	11-1
Overview: Default Restriction Tables	11-1
Creating Restriction Tables	11-1

Modifying Restriction Tables 11-2

Deleting Restriction Tables 11-3

CHAPTER 12

Setting Up System Transfers 12-1

System Transfer Overview 12-1

Task List: Offering Caller System Transfers 12-2

Configuring a Greeting to Allow System Transfers 12-3

Task List: Offering User System Transfers 12-3

CHAPTER 13

Cisco Unity Connection Conversation 13-1

How Outside Callers Interact With Cisco Unity Connection by Phone 13-1

How Users Interact With Cisco Unity Connection by Phone 13-1

How Administrators Can Customize the User Conversation 13-2

Advanced Conversation Configuration Settings 13-2

Customizing the Language of System Prompts 13-2

Class of Service Settings 13-2

User Account and Template Settings 13-3

Using the Custom Keypad Mapping Tool 13-4

How Users Can Customize the User Conversation 13-5

CHAPTER 14

Changing Conversation Settings for All Users 14-1

Accessibility Settings in Effect During the Password Entry Conversation 14-1

Addressing Priority Lists 14-2

Addressing and Recording Order 14-3

Call Waiting Hold Time 14-3

Caller Information 14-4

Dial Prefix Settings for Live Reply to Unidentified Callers 14-5

Deleting Messages 14-5

Language of System Prompts 14-6

Logging On to Cisco Unity Connection from a User Greeting 14-7

Requesting Users Re-Enter Only the Password After a Failed Password Entry 14-8

Saving Speed and Volume Changes Made by Users 14-9

Skipping Messages: Saving New Messages 14-9

Voice Recognition: Allowing Users to Say Their Voice Mail Passwords 14-10

Voice Recognition: Confirmation Confidence Threshold 14-11

Voice Recognition: Global Nickname List 14-12

Additional Advanced Conversation Configuration Settings 14-13

CHAPTER 15

Custom Keypad Mapping Tool 15-1

Using the Custom Keypad Mapping Tool 15-1

Guidelines for Assigning Keys to Menu Options 15-2

Setting a Keypad Mapping to Match an Existing Conversation Mapping 15-2

Conversation Menus That Can Be Customized 15-3

Main Menu Tab 15-3

Message Playback Menu Tabs (Message Header Tab, Message Body Tab, and Message Footer Tab) 15-4

After Message Menu Tab 15-9

Settings Menu Tab 15-11

Message Settings Menu Tab 15-12

Personal Settings Menu Tab 15-12

Documenting Your Keymap 15-13

CHAPTER 16

Changing the Audio Format of Recordings and Media Streams 16-1

Changing the Audio Format That Cisco Unity Connection Uses for Calls 16-1

Changing the Audio Format for Recordings 16-2

CHAPTER 17

Managing Recorded Greetings and Recorded Names 17-1

Using the Media Master to Record Greetings and Names 17-1

Using the Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings 17-2

Setting Up the Cisco Unity Greetings Administrator 17-4

Changing the Audio Format for Recording Greetings and Names 17-5

CHAPTER 18

Specifying Password, Logon, and Lockout Policies 18-1

Cisco Unified Communications Manager Business Edition (CMBE) Only 18-1

Cisco Unity Connection Only 18-1

Specifying Password, Logon, and Lockout Policies by Using Authentication Rules (Cisco Unity Connection Only) 18-2

Creating and Modifying Authentication Rules, and Assigning Rules to Users (Cisco Unity Connection Only) 18-2

CHAPTER 19

Messaging 19-1

Types of Messages 19-1

Message Recording 19-4

Configuring the Termination Warning Prompt for the End of Recording 19-5

Default Recipient Accounts	19-5
Dispatch Messages	19-6
Dispatch Messaging Limitations and Behavioral Notes	19-7
Message Delivery	19-9
How Cisco Unity Connection Handles Messages That Cannot Be Delivered	19-9
How Cisco Unity Connection Handles Messages When System Components Are Unavailable	19-9
How Cisco Unity Connection Handles Messages That Are Interrupted by Disconnected Calls	19-10
How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded	19-11
How Cisco Unity Connection Handles Messages When Maximum Mailbox Store Size Is Exceeded	19-11
Message Delivery and Sensitivity Options	19-12
Message Actions	19-13
Message Subject Line Formats	19-13
Subject Line Parameters	19-14
Subject Line Format Examples	19-16
Subject Line Format Configuration	19-16
Message Storage	19-17
Message Access	19-17
Configuring Live Record	19-18
Configuring Access to RSS Feeds of Voice Messages	19-20
Allowing Insecure Connections to RSS Feeds	19-20
Configuring an RSS Reader to View Voice Messages	19-21
RSS Feed Limitations and Behavioral Notes	19-21

CHAPTER 20

Configuring IMAP Settings 20-1

SMTP Message Handling Overview	20-1
Integrated Messaging Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook	20-2
Recommendations for Deploying IMAP Access	20-3
Task List for Configuring IMAP Access in Cisco Unity Connection	20-3
Procedures for Configuring IMAP Access in Cisco Unity Connection	20-4
Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host	20-4
Configuring Message Relay Settings (Cisco Unity Connection 7.1 and Later)	20-5
Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication	20-5
Configuring SMTP Message Parameters	20-7

CHAPTER 21

Managing Mailbox Stores 21-1

How Multiple Mailbox Stores Work	21-1
----------------------------------	------

Replication	21-2
User Templates	21-2
Maximum Size of a Mailbox Store	21-2
Backups with Multiple Mailbox Stores	21-3
Creating a Mailbox Store	21-4
Moving Mailboxes Between Mailbox Stores	21-4
Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged	21-5
Deleting a Mailbox Store	21-5
Disabling and Re-Enabling a Mailbox Store	21-7

CHAPTER 22**Controlling the Size of Mailboxes 22-1**

Specifying Mailbox Size Quotas	22-1
Changing the Message Aging Policy	22-2

CHAPTER 23**Setting Up SMTP and SMS (SMPP) Message Notifications 23-1**

Setting Up SMTP Message Notifications	23-1
Setting Up SMS (SMPP) Message Notifications	23-2
Task List for Setting Up SMS (SMPP) Message Notifications	23-3

CHAPTER 24**Securing User Messages: Controlling Access and Distribution 24-1**

How Cisco Unity Connection Handles Messages That Are Marked Private or Secure	24-1
Disabling the “Save Recording As” Option in the Media Master for All Voice Messages	24-3
Message Security Options for IMAP Client Access	24-3

CHAPTER 25**Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection 25-1**

Deciding Whether to Create and Install an SSL Certificate	25-1
Creating and Installing an SSL Server Certificate	25-2

CHAPTER 26**Setting Up Broadcast Messaging 26-1**

How System Broadcast Messages Work	26-1
Task List for Offering Broadcast Messaging to Users	26-2
Enabling Phone Access to the Broadcast Message Administrator	26-2
Creating a Call Handler to Send Users to the Broadcast Message Administrator	26-3
Setting Up a One-Key Dialing Option to Send Users to the Broadcast Message Administrator	26-3
Setting Up a Special Phone Number and Routing Rule to Send Users to the Broadcast Message Administrator	26-5
Using the Broadcast Message Administrator	26-5

[Changing Broadcast Message Administrator Defaults](#) 26-6

CHAPTER 27

[Managing System Distribution Lists](#) 27-1

[Predefined System Distribution Lists](#) 27-1

[Creating System Distribution Lists](#) 27-2

[Modifying System Distribution Lists](#) 27-3

[Managing System Distribution List Members](#) 27-3

[Adding Alternate Names for a System Distribution List](#) 27-4

CHAPTER 28

[Managing Partitions and Search Spaces](#) 28-1

[Overview: Partitions](#) 28-1

[Overview: Search Spaces](#) 28-2

[Default Partition and Search Space](#) 28-2

[Search Space Examples](#) 28-3

[Single Site Automated Attendant Search Space Example](#) 28-3

[Multiple Site Search Space Example](#) 28-4

[How Search Spaces Work in Cisco Unity Connection](#) 28-5

[Search Spaces and Users](#) 28-5

[Search Spaces and Call Routing Rules](#) 28-6

[Search Spaces and System Distribution Lists](#) 28-6

[Search Spaces and System Call Handlers](#) 28-7

[Search Spaces and Directory Handlers](#) 28-7

[Search Spaces and Interview Handlers](#) 28-7

[Search Spaces and Digital Networking](#) 28-7

[Search Spaces and VPIM Locations](#) 28-8

[Search Spaces and System Contacts](#) 28-8

[Managing Partitions](#) 28-8

[Managing Search Spaces](#) 28-9

[Changing the System Default Partition and Search Space](#) 28-11

[Finding Objects that Belong to a Partition or Search Space](#) 28-11

[Finding Objects Based on Partition in Cisco Unity Connection Administration](#) 28-11

[Finding Users Based on Partition in Cisco Unity Connection Serviceability](#) 28-12

[Finding Users Based on Partition or Search Space in the Cisco Unity Connection Bulk Edit Utility](#) 28-12

CHAPTER 29

[Managing the Phone System Integrations](#) 29-1

[Managing Phone Systems](#) 29-1

[Adding a New Phone System Integration](#) 29-2

Deleting a Phone System Integration	29-2
Changing Phone System Settings	29-3
Listing the Users Who Are Associated with the Phone System	29-3
Disabling the Use of the Same Port for Turning On and Off an MWI	29-3
Synchronizing MWIs for the Phone System	29-4
Configuring Phone View Settings (Cisco Unified Communications Manager Integrations Only)	29-4
Changing Call Loop Detection Settings	29-4
Managing AXL Servers	29-5
Managing Port Groups	29-7
Adding a Port Group	29-8
Deleting a Port Group	29-9
Changing Port Group Settings	29-9
Changing the Audio Format That Cisco Unity Connection Uses for Calls	29-9
Changing MWI Settings	29-10
Adding Secondary Cisco Unified Communications Manager Servers	29-10
Deleting Cisco Unified Communications Manager Servers	29-11
Changing Cisco Unified Communications Manager Server Settings	29-11
Adding a TFTP Server	29-12
Deleting a TFTP Server	29-12
Changing TFTP Server Settings	29-13
Adding a SIP Server	29-13
Deleting a SIP Server	29-14
Changing SIP Server Settings	29-14
Managing PIMG/TIMG Units	29-15
Changing Session Initiation Protocol (SIP) Settings	29-16
Changing Port Group Advanced Settings	29-16
Changing Automatic Gain Control (AGC) Settings	29-17
Managing Ports	29-17
Adding a Port	29-17
Deleting a Port	29-18
Changing Port Settings	29-18
Viewing the Port Certificate	29-20
Managing Phone System Trunks	29-20
Adding a Phone System Trunk	29-21
Deleting a Phone System Trunk	29-21
Changing Phone System Trunk Settings	29-21
Security (Cisco Unified Communications Manager Integrations Only)	29-22
Viewing the Cisco Unity Connection Root Certificate	29-22
Saving the Cisco Unity Connection Root Certificate as a File	29-23

Adding a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-23
Deleting a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-24
Changing a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-24
Adding a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-25
Deleting a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-25
Changing a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)	29-25

CHAPTER 30

Creating a Cisco Unified Mobility Advantage Integration 30-1

About the Cisco Unified Mobility Advantage Integration	30-1
Task List for Creating an Integration with Cisco Unified Mobility Advantage	30-1
Requirements	30-2
Configuring Cisco Unity Connection	30-2
Testing the Integration with Cisco Unified Mobility Advantage	30-3

CHAPTER 31

Setting Up Phone View 31-1

CHAPTER 32

Creating a Cisco Fax Server Integration 32-1

About the Cisco Fax Server Integration	32-1
Task List for Creating a Cisco Fax Server Integration	32-2
Requirements	32-2
Configuring the Cisco Fax Server	32-2
Configuring Cisco Unity Connection	32-5
Configuring Users	32-7
Testing the Cisco Fax Server Integration	32-7
Changing the Cisco Unity Connection Configuration for the Cisco Fax Server Integration	32-8
Changing the User Configuration for the Cisco Fax Server Integration	32-9
Configuring a Single Number to Receive Both Voice Calls and Faxes	32-9
Task List	32-9
Requirements	32-10

CHAPTER 33

Using Digital Networking 33-1

Setting Up Cisco Unity Connection to Use Digital Networking	33-2
Prerequisites	33-2

Task List	33-2
Procedures for Setting Up Cisco Unity Connection to Use Digital Networking	33-3
Making Deployment Decisions and Gathering Needed Information	33-4
Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain	33-5
Joining Two Cisco Unity Connection Servers to Create a Digital Network	33-6
Adding a Cisco Unity Connection Server to an Existing Network	33-8
Checking Replication Status	33-9
Configuring a Smart Host	33-10
Configuring SMTP Access for Cluster Subscriber Servers	33-11
Configuring Search Spaces for Digital Networking	33-12
Securing the Digital Networking Setup	33-13
Configuring Cross-Server Logon and Transfers	33-13
Testing the Digital Networking Setup	33-14
Creating a Network-Wide All Voice Mail Users Distribution List	33-16
Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts	33-17
Manually Synchronizing Locations	33-17
Removing a Location From the Network	33-18
Digital Networking Concepts and Definitions	33-19
Cisco Unity Connection Locations and Digital Networking	33-19
Object Replication	33-20
Addressing Options for Non-Networked Phone Systems	33-21
Identified User Messaging Between Networked Cisco Unity Connection Users	33-22
Cross-Server Logon and Transfers	33-23
System Distribution Lists	33-23
Private Distribution Lists	33-24
VPIM Locations and Digital Networking	33-24
Notable Behavior	33-24
Broadcast Messages	33-25
Client Access to Digitally Networked Cisco Unity Connection Servers	33-25
Mapping Users to Cisco Unity Connection Systems	33-25
Replication During Bulk Operations	33-25
Replication with Cisco Unity Connection Clusters	33-25

CHAPTER 34

Using VPIM Networking 34-1

Setting Up Cisco Unity Connection to Use VPIM Networking	34-1
Prerequisites	34-2
Task List: Setting Up Cisco Unity Connection to Use VPIM Networking	34-2
Procedures for Setting Up Cisco Unity Connection to Use VPIM Networking	34-3

Making Design Decisions and Gathering Needed Information	34-3
Determining the Domain Name	34-4
Resolving Names with IP Addresses	34-4
Verifying Connectivity with the Remote Voice Messaging System	34-5
Creating VPIM Locations	34-5
Customizing VPIM Locations	34-6
Creating VPIM Contacts	34-6
Customizing VPIM Contact Directory Update Settings	34-11
Adding Alternate Names for Each VPIM Location	34-13
Gathering Information About Cisco Unity Connection to Configure Another Voice Messaging System for VPIM	34-14
Deleting VPIM Contacts	34-14
Removing a VPIM Location	34-15
VPIM Concepts	34-15
VPIM Messages	34-16
VPIM Addresses	34-17
Message Addressing Options	34-17
Messaging Similarities and Limitations	34-17
Audio Format Considerations	34-18

CHAPTER 35

Creating Calendar Integrations 35-1

About Calendar Integrations	35-1
Creating a Calendar Integration with Exchange 2007	35-1
Task List for Creating a Calendar Integration with Exchange 2007	35-2
Requirements for the Exchange 2007 Calendar Integration	35-2
Configuring Exchange 2007 for the Calendar Integration	35-3
Configuring Cisco Unity Connection for the Exchange 2007 Calendar Integration	35-5
Configuring Users for the Exchange 2007 Calendar Integration	35-6
Testing the Exchange 2007 Calendar Integration	35-7
Changing the Cisco Unity Connection Configuration for the Exchange 2007 Calendar Integration	35-8
Changing the User Configuration for the Exchange 2007 Calendar Integration	35-8
Creating a Calendar Integration with Exchange 2003	35-10
Task List for Creating a Calendar Integration with Exchange 2003	35-10
Requirements for the Exchange 2003 Calendar Integration	35-10
Configuring Exchange 2003 for the Calendar Integration	35-11
Configuring Cisco Unity Connection for the Exchange 2003 Calendar Integration	35-14
Configuring Users for the Exchange 2003 Calendar Integration	35-15
Testing the Exchange 2003 Calendar Integration	35-16

Changing the Cisco Unity Connection Configuration for the Exchange 2003 Calendar Integration	35-16
Changing the User Configuration for the Exchange 2003 Calendar Integration	35-17
Creating a Calendar Integration with Cisco Unified MeetingPlace	35-18
Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace	35-18
Requirements for the Cisco Unified MeetingPlace Calendar Integration	35-19
Configuring Cisco Unified MeetingPlace for the Calendar Integration	35-19
Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration	35-20
Configuring Users for the Cisco Unified MeetingPlace Calendar Integration	35-21
Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration	35-23
Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Calendar Integration	35-23
Changing the User Configuration for the Cisco Unified MeetingPlace Calendar Integration	35-24
Creating a Calendar Integration with Cisco Unified MeetingPlace Express	35-25
Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace Express	35-25
Requirements for the Cisco Unified MeetingPlace Express Calendar Integration	35-26
Configuring Cisco Unified MeetingPlace Express for the Calendar Integration	35-26
Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration	35-27
Configuring Users for the Cisco Unified MeetingPlace Express Calendar Integration	35-29
Testing the Cisco Unified MeetingPlace Express Calendar Integration	35-30
Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Express Calendar Integration	35-30
Changing the User Configuration for the Cisco Unified MeetingPlace Express Calendar Integration	35-32

CHAPTER 36**Configuring Service Parameters 36-1**

Configuring Service Parameters for a Cisco Unified Serviceability Service	36-1
Description of Service Parameters	36-2

CHAPTER 37**Configuring Enterprise Parameters 37-1**

Configuring Enterprise Parameters for Cisco Unified Serviceability Services	37-1
Description of Enterprise Parameters	37-2

CHAPTER 38**Installing Plugins 38-1****CHAPTER 39****Managing Descriptions of Message Attachments 39-1**

Adding a Description of a Message Attachment	39-1
Changing a Description of a Message Attachment	39-2

Deleting a Description of a Message Attachment 39-2

CHAPTER 40

Configuring Access to Emails in an External Message Store 40-1

About User Access to Emails in an External Message Store 40-1

Configuring Access to Emails in an Exchange 2007 Message Store 40-1

Task List for Offering Users Access to Exchange 2007 Emails 40-2

Enabling IMAP Access to Exchange 40-2

Configuring Secure IMAP with SSL and Enabling the SSL Certificate (Exchange 2007 Only) 40-3

Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access 40-4

Configuring Users for the External Services 40-5

Configuring Access to Emails in an Exchange 2003 Message Store 40-5

Task List for Offering Users Access to Exchange 2003 Emails 40-6

Enabling IMAP Access to Exchange 40-7

Creating and Configuring an Active Directory Service Account (Exchange 2003 Only) 40-7

Creating and Installing SSL Certificates (Exchange 2003 Only) 40-8

Requiring Secure Communication Between Cisco Unity Connection and Exchange (Exchange 2003 Only) 40-12

Configuring the Cisco Unity Connection Server to Trust Exchange Certificates (Exchange 2003 Only) 40-13

Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access 40-15

Configuring Users for the External Services 40-15

CHAPTER 41

Generating Reports 41-1

Reports Overview 41-1

Setting Report Configuration Parameters 41-4

Archiving Report Data 41-5

Generating and Viewing Reports 41-5

CHAPTER 42

Configuring and Customizing a Cisco Unity Connection Cluster 42-1

CHAPTER 43

Integrating Cisco Unity Connection with an LDAP Directory 43-1

Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users 43-2

Activating the Cisco DirSync Service 43-3

Enabling LDAP Synchronization 43-3

Converting Phone Numbers into Extensions 43-4

Uploading SSL Certificates on the Connection Server 43-4

Configuring LDAP Authentication	43-5
Filtering LDAP Users	43-6
Adding LDAP Configurations and Synchronizing Data	43-7

CHAPTER 44

Managing Licenses	44-1
About License Files	44-1
License Files and MAC Addresses	44-1
Cisco Unity Connection Can Use Multiple Installed License Files	44-2
License Files Must Be Installed	44-2
Permanent, Time-Expiring, and Demonstration License Files	44-2
License Files and Cisco Unity Connection Clusters	44-2
Obtaining and Installing a License File	44-2
Viewing Reports for Licenses	44-4
Viewing the License Usage	44-5
Viewing the License Expirations	44-5
License Parameters for Cisco Unity Connection Features	44-6

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 securing user messages; for managing user passwords; for using VPIM and Digital networking; 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*.

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: <ul style="list-style-type: none">• Key and button names. (Example: Click OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In 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 Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/roadmap/7xcucdg.html.

Obtaining Documentation and Submitting a Service Request

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

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

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

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.



CHAPTER 1

Configuring the Browser on an Administrator Workstation

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

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

- [Firefox, page 1-1](#)
- [Microsoft Internet Explorer, page 1-2](#)

Firefox

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 the applicable System Requirements document:
 - *System Requirements for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html
 - *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucmbesysreqs.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.)

Microsoft Internet Explorer

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 of the applicable System Requirements document:
 - *System Requirements for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html
 - *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucmbesysreqs.html
2. 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 Connection server to the Trusted Sites list by doing the following procedure.

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 Login page. It is not necessary to log in to the Cisco PCA. |
| Step 2 | On the Internet Explorer File menu, click Add This Site To > Trusted Sites Zone . |
| Step 3 | In the Trusted Sites dialog box, click Add . |
| Step 4 | Click Close to close the Trusted Sites dialog box. |
| Step 5 | Restart Internet Explorer. |
-



CHAPTER 2

Accessing and Using Cisco Unity Connection Administration

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, page 2-1](#)
- [Cisco Unity Connection Administration User Interface, page 2-2](#)
- [Using Cisco Unity Connection Administration Help, page 2-2](#)
- [Finding Records in Cisco Unity Connection Administration, page 2-3](#)

For information on configuring the browser on the administrator workstation, see the “[Configuring the Browser on an Administrator Workstation](#)” chapter.

Accessing and Exiting Cisco Unity Connection Administration

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

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

To Log On 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 Connection Administration. If a Connection cluster is configured, we recommend that you bookmark this page for both Connection servers so that you can log on to Connection Administration on the functional server when the other Connection server is not functioning.

- Step 3** Enter an applicable user name and password, and click **Login**.

To Exit Cisco Unity Connection Administration

- Step 1** In the Cisco Unity Connection Administration title pane, click **Logout**.
- Step 2** Exit the web browser.
-

Cisco Unity Connection Administration 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 Connection Administration pages. Click the name of the page to display it.
Title pane	Located across top of the interface; contains an About link and the Log Off link. The title pane also offers a Navigation menu that you can use to browse to other Cisco applications. Click the name of the application from the Navigation list, and then click Go. Depending on the application, you may be required to log on.
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 click a page in the navigation path to go that page.
Page	Where 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 Help

To access Help, click 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	<p>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 Connection Administration. In most cases there are cross-references to additional topics related to the current page.</p> <p>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.</p>

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

Finding Records in Cisco Unity Connection Administration

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. 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. Connection saves your Rows Per Page setting, so that on subsequent logons 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 click **Users**.
 - Step 2** On the Search Users page, in the Search Results table, click 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 click **Find**.
 - Step 4** In the Search Results table, click 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, click 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. Click **Find**.
 - Step 4** In the Search Results table, click the record name to display the record.
-



CHAPTER 3

Administrative Tools

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 Connection web applications, see the [“Configuring the Browser on an Administrator Workstation”](#) chapter.)

See the following sections:

- [Application Plug-ins, page 3-1](#)
- [Cisco Object Backup and Restore Application Suite \(COBRAS\), page 3-2](#)
- [Cisco Unity Connection Administration, page 3-2](#)
- [Cisco Unity Connection Bulk Administration Tool, page 3-2](#)
- [Cisco Unity Connection Bulk Edit Utility, page 3-3](#)
- [Cisco Unity Connection Custom Keypad Mapping Tool, page 3-4](#)
- [Cisco Unity Connection Grammar Statistics Tool, page 3-4](#)
- [Cisco Unity Connection Import and Synch Users Tools, page 3-4](#)
- [Cisco Unity Connection Migrate Messages Utility, page 3-5](#)
- [Cisco Unity Connection Migrate Users Utility, page 3-6](#)
- [Cisco Unity Connection Serviceability, page 3-6](#)
- [Cisco Unity Connection Task Management Tool, page 3-7](#)
- [Disaster Recovery System, page 3-7](#)
- [Cisco Voice Technology Group Subscription Tool, page 3-7](#)
- [Real-Time Monitoring Tool, page 3-7](#)
- [Cisco Unified Serviceability, page 3-8](#)
- [Remote Database Administration Tools, page 3-8](#)
- [Cisco Utilities Database Link for Informix \(CUDLI\), page 3-10](#)
- [Connection User Data Dump \(CUDD\), page 3-10](#)
- [Wallet Card Wizard, page 3-10](#)

Application Plug-ins

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 coresident configurations, see the *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html for detailed information.

For standalone configurations, see the “Installing Plugins” chapter for detailed information.

Cisco Object Backup and Restore Application Suite (COBRAS)

Revised May 2009



Note

The information in this section is not applicable to Cisco Unified Communications Manager Business Edition.

Cisco Object Backup and Restore Application Suite (COBRAS) is the application you use to migrate data and messages from Cisco Unity or from Cisco Unity Connection 1.x to Connection 7.x. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/App_COBRAS.htm.

Alternatively, you can use the Cisco Unity Connection Migrate Messages and Migrate Users utilities to migrate messages and user data. However, we recommend that you use these utilities only 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 Migrate Messages Utility” section on page 3-5 and the “Cisco Unity Connection Migrate Users Utility” section on page 3-6.

For a task list that enumerates the steps for migrating from Cisco Unity or from Connection 1.x to Connection 7.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the applicable chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrugx.html.

Cisco Unity Connection Administration

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” chapter.

Cisco Unity Connection Bulk Administration Tool

The Cisco Unity Connection Bulk Administration Tool (BAT) can be used as follows:

- In standalone configurations, the BAT allows you to create, update, and delete multiple user accounts or system contacts 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 or system contacts from Cisco Unity Connection to a CSV file.

- In coresident configurations, the BAT allows you to create and delete multiple system contacts at the same time by importing information contained in a comma separated value (CSV) file. (To update multiple user accounts at once, you must use the BAT available in the Cisco Unified CM Administration.) In addition, it allows you to export information about users or system contacts from Cisco Unity Connection to a CSV file.
- In both standalone and coresident configurations in which Connection data is synchronized with data in an LDAP directory, the BAT allows you to create large numbers of user accounts at the same time by importing information contained in a comma separated value (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 Connection users from users in an LDAP directory. See the “[Cisco Unity Connection 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** Click **Bulk Administration Tool**.
-

For information on using the Connection BAT, see the “[Using the Cisco Unity Connection Bulk Administration Tool](#)” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For information on using the BAT in Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager Bulk Administration Guide*, available at http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html.

Cisco Unity Connection Bulk Edit Utility

The Cisco Unity Connection Bulk Edit utility allows you to select large numbers of user accounts or call handlers and quickly make the same changes to all of them at one time.

To Access the Cisco Unity Connection Bulk Edit Utility

-
- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Click **Bulk Edit**.
-

For information on using the tool, see the following, as applicable:

- To learn how to use Bulk Edit to modify user accounts, see the “[Setting Up Features and Functionality That Are Controlled by User Account Settings](#)” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
- To learn how to use Bulk Edit to modify call handlers, see the “[Managing Call Handlers](#)” chapter.

Cisco Unity Connection 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** Click **Custom Keypad Mapping**.
-

For information on using the tool, see the [“Custom Keypad Mapping Tool”](#) chapter.

Cisco Unity Connection 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, user names and alternate names, distribution list names, and so on). When administrators add or change names on the 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, 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 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 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 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 click the Rebuild Grammars button on the Grammar Statistics tool.

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

In coresident 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 **Tools**.
- Step 2** Click **Import Users** or **Synch Users**, as applicable.
-

For information on using both tools, see the “[Creating Multiple User Accounts from Cisco Unified Communications Manager Users](#)” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Cisco Unity Connection Migrate Messages Utility

Revised May 2009



Note

The information in this section is not applicable to Cisco Unified Communications Manager Business Edition.

To migrate messages and data from Cisco Unity 4.0(5) or later or from Cisco Unity Connection 1.x to Connection 7.x, we recommend that you use the Cisco Object 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/App_COBRAS.htm.

For a task list that enumerates the steps for migrating from Cisco Unity or from Connection 1.x to Connection 7.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the applicable chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrugx.html.

The Cisco Unity Connection Migrate Messages utility allows you to migrate messages from Cisco Unity or from Cisco Unity Connection 1.x to Cisco Unity Connection 7.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 (Standalone Configurations Only)

-
- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Expand **Migration Utilities**, then click **Migrate Users**.
-

Cisco Unity Connection Migrate Users Utility

Revised May 2009

**Note**

The information in this section is not applicable to Cisco Unified Communications Manager Business Edition.

To migrate messages and data from Cisco Unity 4.0(5) or later or from Cisco Unity Connection 1.x to Connection 7.x, we recommend that you use the Cisco Object 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/App_COBRAS.htm.

For a task list that enumerates the steps for migrating from Cisco Unity or from Connection 1.x to Connection 7.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the applicable chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/upgrade/guide/7xcucrux.html.

To Access the Migrate Users Utility (Standalone Configurations Only)

-
- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Expand **Migration Utilities**, then click **Migrate Users**.
-

Cisco Unity Connection Serviceability

Revised May 2009

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

- Displaying Connection alarm definitions, which you can use for troubleshooting.
- Enabling 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 Connection trace information is saved.
- Viewing and changing the server status of the Connection servers when a Connection cluster is configured.
- Viewing the status of the Connection feature services.
- Activating, deactivating, starting, and stopping the 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 7.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/serv_administration/guide/7xcucservagx.html.

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

To Access the Task Management Tool

-
- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Click **Task Management**.
-

Disaster Recovery System

Disaster Recovery System lets you back up and, if necessary, restore data and voice messages on a Cisco Unity Connection or Cisco Unified CMBE system. For more information, see the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsa.html.

Cisco Voice Technology Group Subscription Tool

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

Revised May 2009

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 Connection.

RTMT allows you to perform the following tasks:

- Monitoring a set of predefined management objects that focus on the health of the system.
- Generating various alerts, in the form of emails, for objects when values go over or below user-configured thresholds.
- Collecting and viewing traces in various default viewers that exist in RTMT.
- Viewing syslog messages and alarm definitions in SysLog Viewer.
- Working with performance-monitoring counters.
- Monitoring the voice messaging ports on Connection. When a Connection cluster is configured, you can open multiple instances of RTMT to monitor voice messaging ports on each server in the 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

Revised September 2008

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 activate, deactivate, 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

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 \(CUDLI\), page 3-10](#)
- [Connection User Data Dump \(CUDD\), page 3-10](#)

- [Wallet Card Wizard, 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 click 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 Connection Database Proxy service is disabled by default.
- A built-in shutdown timer disables the Connection Database Proxy service after a configurable number of days.

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 Change the Database Proxy Service Shutdown Timer, page 3-9](#)
- [To Start the Database Proxy Service, page 3-10](#)

To Assign the Remote Administrator Role to One or More Users

Step 1 In Cisco Unity Connection Administration, click **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, click **Roles**.

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

Step 5 Click **Save**.

Step 6 Repeat [Step 2](#) through [Step 5](#) for each user who needs access to remote administration tools.

To Change the Database Proxy Service Shutdown Timer

Step 1 In Cisco Unity Connection Administration, click **System Settings > Advanced > Connection Administration**.

Step 2 In the Database Proxy: Service Shutdown Timer field, enter a value between 1 and 999 days. A value of zero disables the Database Proxy Service.

Step 3 Click **Save**.

To Start the Database Proxy Service

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

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

Cisco Utilities Database Link for Informix (CUDLI)

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/App_CUDLE_LL.htm.

Connection User Data Dump (CUDD)

The 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/APP_UserDataDump.htm.

Wallet Card Wizard

Added May 2009

The Wallet Card wizard is available for producing a PDF file of a wallet card based on any of the Connection conversations, including custom keypad mappings. The templates in the wizard list frequently used menu options and shortcuts for managing 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 logging on to Connection. The Wallet Card wizard is a Windows-based remote database administration tool.

Download the tool and view Help at
http://www.ciscounitytools.com/App_CUC_WalletCardWizard.htm.



CHAPTER 4

Call Management Overview

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, page 4-1](#)
- [Call Handlers, page 4-2](#)
- [Directory Handlers, page 4-2](#)
- [Interview Handlers, page 4-3](#)
- [Call Routing Tables, page 4-3](#)
- [Restriction Tables, page 4-6](#)
- [Schedules and Holidays, page 4-8](#)
- [Default Cisco Unity Connection Automated Attendant Behavior, page 4-9](#)

After reading about call management concepts, see the “[Creating a Call Management Plan](#)” chapter for instructions on developing a plan.

Overview of Call Management Concepts

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 directory assistance 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 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 Connection, or add new objects and combine them to create the caller experience.

Call Handlers

Revised May 2009

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 2,500 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 cell phone of the person who is on call), or to another call handler.

To learn how to create and customize call handlers, see the [“Managing Call Handlers”](#) chapter.

Directory Handlers

Revised May 2009

Directory handlers provide directory assistance 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 user name 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	<p><i>(For Cisco Unity Connection systems with the voice-recognition option only).</i> For this type of directory handler, callers say the first name and last name of the 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.</p> <p>Connection users who are listed in the directory are available to outside callers as names that can be reached. System contacts are only available to Connection users who are logged on to Connection, and personal contacts are only available to the Connection users who defined them.</p> <p>Note that 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.</p>

To learn how to create and customize directory handlers, see the [“Managing Directory Handlers”](#) chapter.

Interview Handlers

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. 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”](#) chapter.

Call Routing Tables

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 logon 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 Connection. The predefined direct routing rules are: <ul style="list-style-type: none">• Attempt Sign-In—Calls from users are routed to the user logon conversation.• Opening Greeting—Calls from outside callers are routed to the Opening Greeting.
Forwarded Rules	Forwarded rules handle calls that are forwarded to 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: <ul style="list-style-type: none">• Attempt Forward—All calls forwarded from a user extension are routed to the user greeting.• 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 4-5 to learn more about routing rules. When you are ready to create and customize them, see the [“Managing Call Routing Tables”](#) chapter.

How Call Routing Rules Work

Revised May 2009

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 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 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 (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 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 ¹	Port ¹	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

1. Applicable to Cisco Unity Connection 7.1 only.

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 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 Connection always play a standard greeting or legal disclaimer to all callers, whether they call 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

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”](#) section on page 12-1.)
- 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.

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 are applied regardless of how a user or administrator accesses Cisco Unity Connection. They do not affect the phone numbers that users can dial when they are not logged on to 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. Because users without mailboxes (typically, administrators) are not assigned to a class of service, Connection applies the default restriction tables (default transfer, default outdial, or default fax) to actions taken by these types of users, including actions taken on behalf of other users.

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”](#) chapter.

How Restriction Tables Work

When a user uses the Cisco Unity Assistant or the Cisco Unity Connection conversation to attempt to change a phone number that is used for call transfer, message notification, or fax delivery, or when users use Caller system transfers to transfer to a number that they specify, Connection applies the applicable restriction table to verify that the phone number entered is allowed. The same thing happens when an

administrator uses Cisco Unity Connection Administration to attempt to change a phone number that is used for message notification or call transfer. In each case, the restriction table used is the one associated with the user or administrator who is changing the number.

For example, if a user uses the Cisco Unity Assistant to enter a phone number to set up a message notification device, 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, Connection applies the default restriction table—in this example, the default outdial table—not the restriction table that is associated with the class of service of the user. Therefore, an administrator can, when necessary, override the limitations of the class of service of a particular user.

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 are permitted for use. The restriction table is applied when a user or an administrator attempts to change a number that is controlled by a restriction table, not when Connection tries to complete a transfer or delivery. To protect Connection from toll fraud and unauthorized use when users use Caller system transfers, users must log on to Connection, enter the number that they want to transfer to, and Connection performs the transfer only when the Default System Transfer restriction table permits it.

When a restriction table is applied to a number (such as a pager number for a message notification), 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, Connection then compares the number with the call pattern in the second dial string, and so on, until it finds a match. When Connection finds a match, it either permits or restricts the use of the number as specified in the dial string.

Restriction tables are commonly used to permit or restrict the use of 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, 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, 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, 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, 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

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.

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	<p>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.)</p> <p>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.</p>
Closed hours	<p>The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.</p> <p>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.</p>
Holidays	<p>When a Holiday setting is in effect, 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.</p> <p>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.</p>

To modify predefined schedules or to create your own, see the [“Managing Schedules and Holidays”](#) chapter.

Default Cisco Unity Connection 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 Connection.

An Outside Caller Calls Cisco Unity Connection During Business Hours

A caller who does not have a Connection mailbox dials the main 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. 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, Connection attempts to match the caller phone number with the extension or alternate extension of a Connection user. When this fails, 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. 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 Connection user, 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, 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, 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, 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 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, Connection should hang up.



CHAPTER 5

Creating a Call Management Plan

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

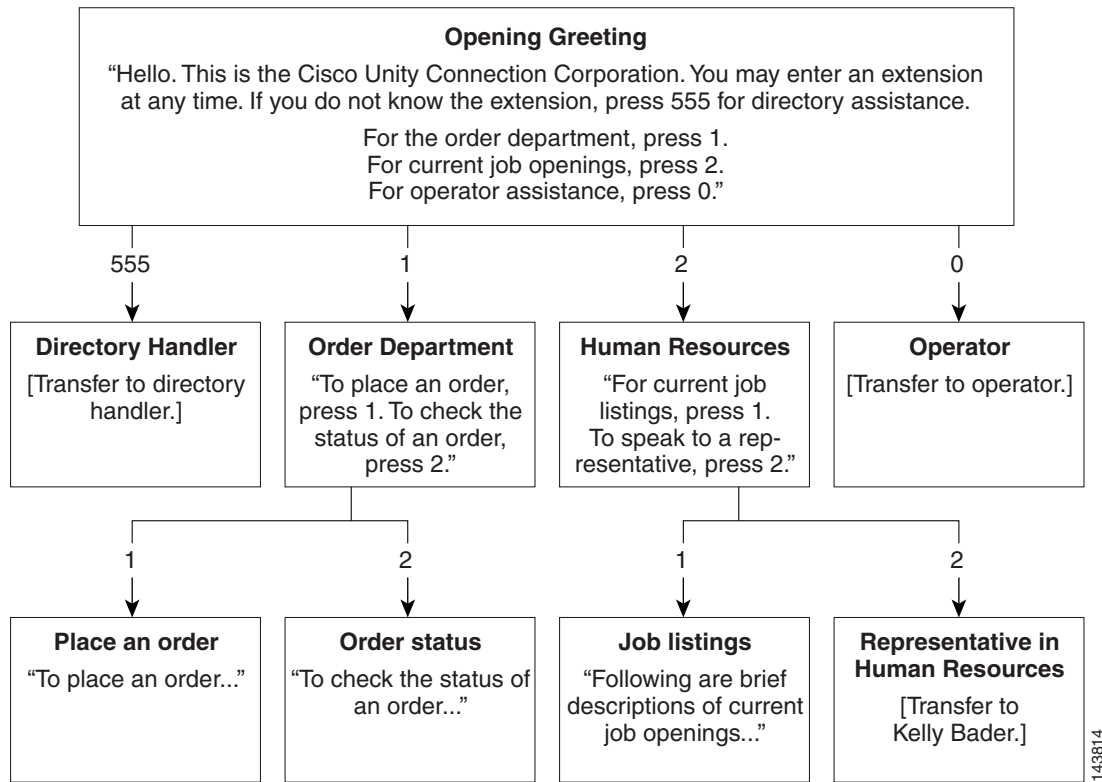
Before beginning the steps in this chapter, make sure you understand each of the system components and call routing elements as described in the [“Call Management Overview”](#) chapter.

See the following sections:

- [Creating a Call Management Map, page 5-1](#)
- [Implementing a Call Management Plan, page 5-2](#)

Creating a Call Management Map

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

143814

Implementing a Call Management Plan

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.



CHAPTER 6

Managing Call Handlers

See the following sections:

- [Overview: Default Call Handlers, page 6-1](#)
- [Creating, Modifying, and Deleting Call Handler Templates, page 6-2](#)
- [Creating Call Handlers, page 6-4](#)
- [Modifying Call Handlers, page 6-4](#)
- [Overview of Call Handler Greetings, page 6-6](#)
- [Managing Call Handler Greetings, page 6-7](#)
- [Managing Caller Input During Greetings, page 6-8](#)
- [Changing Phone Language Settings, page 6-11](#)
- [Taking Messages, page 6-11](#)
- [Transferring Calls, page 6-12](#)
- [Deleting Call Handlers, page 6-12](#)

Overview: Default Call Handlers

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	<p>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.</p> <p>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.</p>
-------------------------	---

Operator	<p>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.</p> <p>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.</p>
Goodbye	<p>Plays a brief goodbye message and then hangs up if there is no caller input.</p> <p>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.</p>

Creating, Modifying, and Deleting Call Handler Templates

Revised May 2009

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. 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 6-3](#)

To Create a Call Handler Template

- Step 1** In Cisco Unity Connection Administration, expand **Templates**, then click **Call Handler Templates**.
- Step 2** On the Search Call Handler Templates page, click **Add New**.
- Step 3** On the New Call Handler Template page, enter basic settings, as applicable. (For field information, on the Help menu, click **This Page**.)



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

- Step 4** Click **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, click **Save**.
- Step 7** On the Edit menu, click 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](#)” section on page 6-12 for details)
 - Caller Input (see the “[Managing Caller Input During Greetings](#)” section on page 6-8 for details)
 - Greetings (see the “[Overview of Call Handler Greetings](#)” section on page 6-6 for details)
 - Message Settings (see the “[Taking Messages](#)” section on page 6-11 for details)
- Step 8** If you change any of the default settings on any of the pages listed in [Step 7](#), click **Save** before leaving the page.

To Modify a Call Handler Template

- Step 1** In Cisco Unity Connection Administration, expand **Templates**, then click **Call Handler Templates**.
- Step 2** On the Search Call Handler Templates page, click 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 click **Find**.

- Step 3** On the Edit Call Handler Template, change settings, as applicable. (For field information, on the Help menu, click **This Page**.)
- Step 4** When you have finished changing settings on the Edit Call Handler Template page, click **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](#)” section on page 6-12 for details)
 - Caller Input (see the “[Managing Caller Input During Greetings](#)” section on page 6-8 for details)
 - Greetings (see the “[Overview of Call Handler Greetings](#)” section on page 6-6 for details)
 - Message Settings (see the “[Taking Messages](#)” section on page 6-11 for details)
- Step 6** If you change any of the settings on a page listed in [Step 5](#), click **Save** before leaving the page.

To Delete a Call Handler Template

- Step 1** In Cisco Unity Connection Administration, expand **Templates**, then click **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 click **Find**.

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

Step 4 Click **OK**.

Creating Call Handlers

Revised May 2009

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 click **System Call Handlers**.

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

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



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

Step 4 Click **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, click **Save**.

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

- Transfer Rules (see the [“Transferring Calls”](#) section on page 6-12 for details)
- Caller Input (see the [“Managing Caller Input During Greetings”](#) section on page 6-8 for details)
- Greetings (see the [“Overview of Call Handler Greetings”](#) section on page 6-6 for details)
- Message Settings (see the [“Taking Messages”](#) section on page 6-11 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](#), click **Save** before leaving the page.


Modifying Call Handlers

Revised May 2009

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 Multiple Call Handlers at Once, page 6-5](#)

To Modify a Single Call Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **System Call Handlers**.
- Step 2** On the Search Call Handlers page, click 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 click **Find**.
- Step 3** On the Edit Call Handler page, change settings as applicable. (For field information, on the Help menu, click **This Page**.)
- Step 4** When you have finished changing settings on the Edit Call Handler page, click **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”](#) section on page 6-12 for details)
 - Caller Input (see the [“Managing Caller Input During Greetings”](#) section on page 6-8 for details)
 - Greetings (see the [“Overview of Call Handler Greetings”](#) section on page 6-6 for details)
 - Message Settings (see the [“Taking Messages”](#) section on page 6-11 for details)
 - Call Handler Owners
- Step 6** If you change any of the settings on a page listed in [Step 5](#), click **Save** before leaving the page.
-

To Modify Multiple Call Handlers at Once

- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Click **Bulk Edit Utility**.
- Step 3** In the Make Changes To section, click **System Call Handlers**.
- Step 4** In the Select Call Handlers list, click the applicable search parameters, and click **Find**.
- Step 5** In the resulting list, check the check boxes adjacent to the call handlers that you want to modify and then click **Next**.
- Step 6** On the applicable tab, check the check boxes of the settings that you want to modify. When you have finished changing settings, click **Next**.
- Step 7** Click **Finish** to apply your changes.
-

Overview of Call Handler Greetings

Revised May 2009

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, 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 that Call Handler greetings can be recorded in multiple languages. See the [“Changing Phone Language Settings” section on page 6-11](#) for instructions.

You can customize how 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, 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 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 that 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. 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. 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. The system default error recording is, “I did not recognize that as a valid entry.” By default, after the error greeting plays, 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”](#) chapter.)

See the following [“Managing Call Handler Greetings”](#) section for instructions on changing call handler greeting settings.

Managing Call Handler Greetings

Revised May 2009

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 6-7](#)
- [To Set Up Call Handler Greetings for Multiple Call Handlers, 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 Cisco Unity Greetings Administrator”](#) section on page 17-4 and the [“Using the Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings”](#) section on page 17-2.

To Set Up Call Handler Greetings for a Single Call Handler

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

Step 2 On the Search Call Handlers page, click 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 click **Find**.

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

Step 4 On the Greetings page, click 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** Click **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

- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Click **Bulk Edit Utility**.
- Step 3** In the Make Changes To section, click **System Call Handlers**.
- Step 4** In the Select Call Handlers list, click the applicable search parameters, and click **Find**.
- Step 5** In the resulting list, check the check boxes adjacent to the call handlers that you want to modify and then click **Next**.
- Step 6** On the Greetings tab, select the settings that you want to modify. When you have finished changing settings, click **Next**.
- Step 7** Click **Finish** to apply your changes.
-

Managing Caller Input During Greetings

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 6-8](#)
- [Offering System Transfers, page 6-9](#)
- [Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter, page 6-10](#)

Offering One-Key Dialing During Call Handler Greetings

Revised May 2009


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, Connection releases 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 click **System Call Handlers**.
- Step 2** On the Search Call Handler page, in the Search Results table, click 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 click **Find**.
-
- Step 3** On the Edit Call Handler page, on the Edit menu, click **Caller Input**.
- Step 4** In the Single Key Settings table, click 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 Connection to immediately process the key without waiting for the caller to enter additional digits.
- Step 6** Under Action, click an option and change settings as applicable.
- Step 7** Click **Save**.
- Step 8** Optionally, you can rerecord the call handler greetings to mention the key that callers can press while listening to the greetings:
- On the Edit menu, click **Greetings**.
 - On the Greetings page, click the display name of the greeting that you want to modify.
 - On the Edit Greeting page, click **Play/Record**, and record a greeting.
 - Click **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 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 Connection users or call handlers while the greeting is playing.

For more information see the [“Setting Up System Transfers”](#) 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, 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, Connection attempts to route the call to extension 1231000; if the prepended extension is not valid, 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, 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 Prepend Digits for Individual User or Call Handler Accounts, page 6-10](#)
- [To Configure Prepend Digits for Multiple User or Call Handler Accounts at Once, page 6-10](#)

To Configure Prepend 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** Click **Save**.
-

To Configure Prepend Digits for Multiple User or Call Handler Accounts at Once


- Step 1** In Cisco Unity Connection Administration, expand **Tools**.
- Step 2** Click **Bulk Edit Utility**.
- Step 3** In the Bulk Edit utility, find the user or call handler accounts that you want to edit. Check the check boxes adjacent to the accounts that you want to modify and then click **Next**.
- Step 4** Click the **Caller Input** tab.
- Step 5** Check the **Prepend Digits to Dialed Extensions** check box and enter the applicable digits.
- Step 6** Click **Next**, and then click **Finish**.
-

Changing Phone Language Settings

Revised May 2009

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 click **System Call Handlers**.
- Step 2** On the Search Call Handler page, in the Search Results table, click 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 click **Find**.
-
- Step 3** On the Edit Call Handler page, click **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the Language list.
- Step 4** Click **Save**.
- Step 5** On the Edit menu, click **Greetings**.
- Step 6** On the Greetings page, click the applicable greeting.
- Step 7** On the Edit Greetings page, rerecord greetings in the new language.
- Step 8** Click **Save**.
-

Taking Messages

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 19-5 for details.

For details on configuring dispatch messages, see the [“Dispatch Messages”](#) section on page 19-6.

Transferring Calls

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, 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, 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, Connection can either release the call to the phone system, or it can supervise the transfer. When Connection is set to supervise transfers, it can provide call screening and call holding options on indirect calls:

- With call screening, 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, Connection can ask callers to hold. Each caller on hold uses a 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, Connection asks whether the caller wants to continue holding, leave a message, or try another extension. 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 Waiting Hold Time”](#) section on page 14-3 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

We recommend that you investigate dependencies among your call handlers prior to deleting one. After you delete a call handler, any call routing rules or other call handlers that directed calls to the call handler instead direct them to the Opening Greeting call handler. 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 click **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 click **Find**.

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



Caution Before deleting the call handler, verify that no routing rules or other call handlers point to it. If other call handlers reference the deleted call handler, be sure to rerecord the greetings of those call handlers and change other settings as necessary to remove mention of the deleted handler.

- Step 4** In the dialog box that asks you to confirm the deletion, click **OK**.



CHAPTER 7

Managing Directory Handlers

Directory handlers provide directory assistance that callers can use to reach Cisco Unity Connection users with mailboxes. When a caller searches for a user name 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: Default Directory Handler, page 7-1](#)
- [Creating a Directory Handler, page 7-1](#)
- [Modifying a Directory Handler, page 7-2](#)
- [Changing Phone Language Settings, page 7-3](#)
- [Routing Calls to a Voice Directory Handler, page 7-3](#)
- [Deleting a Directory Handler, page 7-4](#)

Overview: Default Directory Handler

Revised May 2009

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”](#) section on [page 4-2](#).)

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

Revised May 2009

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 that 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 click **Directory Handlers**.
- Step 2** On the Search Directory Handlers page, click **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** Click **Save**.
- Step 6** On the Edit Directory Handler Basics page, continue entering settings for the directory handler. (For field information, on the Help menu, click **This Page**.)
- Step 7** When you have finished entering settings on the Edit Directory Handler page, click **Save**.
- Step 8** On the Edit menu, click **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, click **Save** before leaving the page.

Modifying a Directory Handler

To Modify a Directory Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Directory Handlers**.
- Step 2** On the Search Directory Handlers page, click 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 click **Find**.

- Step 3** On the Edit Directory Handler Basics page, change settings as applicable. (For field information, on the Help menu, click **This Page**.)
- Step 4** When you have finished changing settings on the Edit Directory Handler page, click **Save**.
- Step 5** To change the settings on the Caller Input page, on the Edit menu, click **Caller Input**.

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

Changing Phone Language Settings

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.

To Change Phone Language Settings for a Directory Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Directory Handlers**.
- Step 2** On the Search Directory Handlers page, click 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 click **Find**.

- Step 3** On the **Edit Directory Handler** page, click **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.
- Step 4** Click **Save**.
-

Routing Calls to a Voice Directory Handler

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

We recommend that you investigate and remove any references to a directory handler prior to deleting it. After you delete a directory handler, any call routing rules or call handlers that directed calls to the directory handler instead direct them to the System Directory Handler. If you delete a directory handler that was previously 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 click **Directory Handlers**.

Step 2 On the Search Directory Handlers page, check 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 click **Find**.

Step 3 Click **Delete Selected**.



Caution Before deleting the directory handler, verify that no routing rules or call handlers point to it. If any call handlers reference the deleted directory handler, be sure to rerecord the greetings of the call handlers and change other settings as necessary to remove mention of the deleted handler.

Step 4 In the dialog box that asks you to confirm the deletion, click **OK**.



CHAPTER 8

Managing Interview Handlers

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, page 8-1](#)
- [Modifying Interview Handlers, page 8-2](#)
- [Changing Phone Language Settings, page 8-2](#)
- [Deleting Interview Handlers, page 8-3](#)

Creating Interview Handlers

To Create an Interview Handler

-
- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Interview Handlers**.
- Step 2** On the Search Interview Handlers page, click **Add New**.
- Step 3** On the New Interview Handler page, enter basic settings, as applicable. (For field information, on the Help menu, click **This Page**.)




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

- Step 4** Click **Save**.
- Step 5** On the Edit Interview Handler page, on the Edit menu, click **Interview Questions**.
- Step 6** On the Interview Questions page, click 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, click **Save** before leaving the page.
-


Modifying Interview Handlers

To Modify an Interview Handler

-
- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Interview Handlers**.
- Step 2** On the Search Interview Handlers page, click 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 click **Find**.
-
- Step 3** On the Edit Interview Handler page, change settings, as applicable. (For field information, on the Help menu, click **This Page**.)
- Step 4** When you have finished changing settings on the Edit Interview Handler page, click **Save**.
- Step 5** On the Edit menu, click **Interview Questions**.
- Step 6** On the Interview Questions page, click 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, click **Save** before leaving the page.
-

Changing Phone Language Settings

To Change Phone Language Settings for an Interview Handler

-
- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Interview Handlers**.
- Step 2** On the Search Interview Handlers page, click 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 click **Find**.
-
- Step 3** On the Edit Interview Handler Basics page, click **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:
- On the Edit menu, click **Interview Questions**.
 - On the Interview Questions page, click a question number.
 - On the Edit Interview Question page, rerecord the question.
- Step 5** As you make changes on the pages, click **Save** before leaving a page.
-

Deleting Interview Handlers

You must investigate and remove any references to an interview handler prior to deleting it. For example, if a caller input key on a call handler sends calls to the interview handler, you must edit the call handler to select a different action. If you delete an interview handler that was previously 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 click **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 click **Find**.

Step 3 Click **Delete Selected**.



Caution Before deleting the interview handler, verify that no routing rules or call handlers point to it. If any call handlers reference the deleted interview handler, be sure to rerecord the greetings of the call handlers and change other settings as necessary to remove mention of the deleted handler.

Step 4 In the dialog box that asks you to confirm the deletion, click **OK**.



CHAPTER 9

Managing Call Routing Tables

See the following sections:

- [Overview: Default Call Routing Rules, page 9-1](#)
- [Adding Call Routing Rules, page 9-2](#)
- [Modifying Call Routing Rules, page 9-2](#)
- [Changing Phone Language Settings, page 9-2](#)
- [Changing the Order of Call Routing Rules, page 9-3](#)
- [Deleting Call Routing Rules, page 9-3](#)

Overview: Default Call Routing Rules

Revised May 2009

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 Connection. The predefined direct routing rules are:

- **Attempt Sign-In**—Calls from users are routed to the user logon conversation.
- **Opening Greeting**—Calls from unidentified callers are routed to the Opening Greeting.

Forwarded rules handle calls that are forwarded to 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.
- **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

To Add a Call Routing Rule

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, click **Direct Routing Rules**. For forwarded calls, click **Forwarded Routing Rules**.
- Step 2** On the Direct Routing Rules or Forwarded Routing Rules page, click **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** Click **Save**.
- Step 5** On the Edit Direct Rule or Edit Forwarded Rule page, continue entering applicable settings. (For field information, on the Help menu, click **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, click **Save**.

Modifying Call Routing Rules

To Modify a Call Routing Rule

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, click **Direct Routing Rules**. For forwarded calls, click **Forwarded Routing Rules**.
- Step 2** On the Direct Routing Rules or Forwarded Routing Rules page, click 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, click **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, click **Save**.

Changing Phone Language Settings

Revised May 2009

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, click **Direct Routing Rules**. For forwarded calls, click **Forwarded Routing Rules**.
- Step 2** On the Direct Routing Rules or Forwarded Routing Rules page, click 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, click **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.
- Step 4** Click **Save**.
-

Changing the Order of Call Routing Rules

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, click **Direct Routing Rules**. For forwarded calls, click **Forwarded Routing Rules**.
- Step 2** On the Direct Routing Rules or Forwarded Routing Rules page, click **Change Order**.
- Step 3** On the Edit Direct Routing Rule Order or Edit Forwarded Routing Rule Order page, in the Reorganization list, click the name of a rule that you want to move, then click the down or up arrow as applicable.
- Step 4** When you have finished reordering the rules, click **Save**.
-

Deleting Call Routing Rules

To Delete a Call Routing Rule

-
- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, click **Direct Routing Rules**. For forwarded calls, click **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** Click **Delete Selected**.
- Step 4** In the dialog box that asks you to confirm the deletion, click **OK**.
-



CHAPTER 10

Managing Schedules and Holidays

See the following sections:

- [Overview: Default Schedules, page 10-1](#)
- [Designating Holidays, page 10-1](#)
- [Creating Schedules, page 10-2](#)
- [Modifying Schedules, page 10-2](#)
- [Deleting Schedules, page 10-3](#)

Overview: Default Schedules

Revised May 2009

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 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 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

Revised May 2009

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 click **Holiday Schedules**.
 - Step 2** On the Search Holiday Schedules page, click **Add New**.
 - Step 3** On the New Holiday Schedule page, enter a display name for the holiday schedule, and click **Save**.
 - Step 4** To add a new holiday to the schedule, on the Edit Holiday Schedule Basics page, click **Add New**.
 - Step 5** On the New Holiday page, enter settings as applicable. (For field information, on the Help menu, click **This Page**.)
 - Step 6** Click **Save**.
 - Step 7** To return to the Edit Holiday Schedule page, on the Edit menu, click **Holiday Schedule Basics**.
-

Creating Schedules

Revised May 2009

To Create a New Schedule

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Schedules**.
 - Step 2** On the Search Schedules page, click **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** Click **Save**.
 - Step 5** To add time frames when the schedule is active, on the Edit Schedule Basics page, in the Schedule Details box, click **Add New**.
 - Step 6** On the New Schedule Detail page, enter settings as applicable. (For field information, on the Help menu, click **This Page**.)
 - Step 7** Click **Save**.
 - Step 8** To return to the Edit Schedule page, on the Edit menu, click **Schedule Basics**.
-

Modifying Schedules

To Modify a Schedule

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Schedules**.
 - Step 2** On the Search Schedules page, click 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 click **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, click **Save**.
- Step 5** To add time frames when the schedule is active, in the Schedule Details box, click **Add New**.
- Step 6** If you change any settings on the New Schedule Detail page, click **Save**. To return to the Edit Schedule page, on the Edit menu, click **Edit Schedule**.
- Step 7** To remove time frames, check the check box next to the schedule detail that you want to remove, and click **Delete Selected**.

**Note**

If you remove all schedule details from a schedule, the schedule is never active. Call handlers that use this schedule as is always use closed hours transfer settings, and the closed greeting always plays (if enabled) for users and call handlers that use this schedule, except when it is overridden by the holiday, internal, busy, or alternate greeting.

Deleting Schedules

To Delete a Schedule

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **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 click **Find**.

- Step 3** Click **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, click **OK**.



CHAPTER 11

Managing Restriction Tables

See the following sections:

- [Overview: Default Restriction Tables, page 11-1](#)
- [Creating Restriction Tables, page 11-1](#)
- [Modifying Restriction Tables, page 11-2](#)
- [Deleting Restriction Tables, page 11-3](#)

Overview: Default Restriction Tables

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 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 Connection user. By default, the table does not allow Connection to dial any numbers.
Default Transfer	Restricts numbers for call transfers.

See the [“How Restriction Tables Work” section on page 4-6](#) for a detailed discussion of how restriction tables function.

Creating Restriction Tables

Revised May 2009

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 click **Restriction Tables**.
- Step 2** On the Search Restriction Tables page, click **Add New**.
- Step 3** On the New Restriction Table page, enter basic settings as applicable. (For field information, on the Help menu, click **This Page**.)




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

- Step 4** Click **Save**.
- Step 5** To add patterns to the restriction table, on the Edit Restriction Table Basics page, in the Restriction Patterns box, click **Add New**.
- Step 6** If you change any settings on the pattern, click **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, click **Change Order**, and then do the following sub-steps:
- To move a pattern within the list, on the Change Restriction Pattern Order page, click the pattern, then click the down or up arrows as applicable.
 - When you have finished reordering the patterns, click **Save**.
 - To return to the Edit Restriction Table page, on the Edit menu, click **Restriction Table Basics**.
- Step 9** To delete a pattern in the list, check the check box to the left of the pattern, click **Delete Selected**, then click **OK** to confirm the deletion.
-

Modifying Restriction Tables



Revised May 2009

To Modify a Restriction Table

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Restriction Tables**.
- Step 2** On the Search Restriction Tables page, click 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 click **Find**.
-
- Step 3** To add patterns to the restriction table, on the Edit Restriction Table Basics page, in the Restriction Patterns box, click **Add New**.
- Step 4** If you change any settings on the pattern, click **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 click **Delete Selected**, then click **OK** to confirm the deletion.
- Step 7** To change the order of the patterns, click **Change Order**, and then do the following sub-steps:
- To move a pattern within the list, on the Change Restriction Pattern Order page, click the pattern, then click the down or up arrows as applicable.
 - When you have finished reordering the patterns, click **Save**.
 - To return to the Edit Restriction Table page, on the Edit menu, click **Restriction Table Basics**.
-

Deleting Restriction Tables

To Delete a Restriction Table

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **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 click **Find**.
-
- Step 3** Click **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, click **OK**.
-



CHAPTER 12

Setting Up System Transfers

See the following sections:

- [System Transfer Overview, page 12-1](#)
- [Task List: Offering Caller System Transfers, page 12-2](#)
- [Task List: Offering User System Transfers, page 12-3](#)

System Transfer Overview

In your organization, you may find that callers want to be able to dial numbers that are not typically listed in directory assistance. 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 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 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 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 Connection users:

Caller System Transfer	<p>This conversation prompts callers to enter the number that they want to transfer to.</p> <p>To help protect your organization from toll fraud and unauthorized use, Connection performs the transfer only when the Default System Transfer restriction table permits it.</p>
User System Transfer	<p>This conversation prompts callers to log on to Connection. After callers enter their Connection IDs and passwords, Connection prompts them to enter the number that they want to transfer to.</p> <p>To help protect your organization from toll fraud and unauthorized use, Connection performs the transfer only when permitted by the transfer restriction table that is associated with the class of service for the user who logged on.</p>

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, 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 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 Connection to offer Caller System Transfers when callers press 3. To offer system transfers to a particular user, you could set 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, 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 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, page 12-2](#)
- [Task List: Offering User System Transfers, page 12-3](#)

When using either the Caller System Transfer or User System Transfer conversation, 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. See the “[Conversation Configuration](#)” section in the “Advanced Settings” chapter of the *Interface Reference Guide for Cisco Unity Connection Administration* for details.

Task List: Offering Caller System Transfers

1. Modify the Default System Transfer restriction table so that callers can dial numbers that you want to allow. See the “[Managing Restriction Tables](#)” 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 12-3.
 - 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 12-3](#)
- [To Configure Multiple Greetings to Allow System Transfers, page 12-3](#)

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** Click **Save**.
-

To Configure Multiple Greetings to Allow System Transfers

-
- Step 1** In Cisco Unity Connection Administration, expand **Tools**, and then click **Bulk Edit Utility**.
- Step 2** In the Bulk Edit utility, find the user or call handler accounts that you want to edit.
- Step 3** Click **Next**.
- Step 4** Click the **Greetings** tab.
- Step 5** On the applicable greeting tab, check the **Allow Transfers to Numbers Not Associated with Users or Call Handlers** check box and click **Yes** in the list.
- Step 6** Repeat [Step 5](#) for each greeting for which you want to allow system transfers.
- Step 7** Click **Next**, and then click **Finish**.
-

Task List: Offering User System Transfers

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 Connection entities. See the [“Managing Restriction Tables”](#) 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”](#) 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.



CHAPTER 13

Cisco Unity Connection Conversation

A Cisco Unity Connection conversation is a set of prerecorded prompts and menu options that callers hear as they interact with Connection by phone. It is organized into two main conversations—one for outside callers and one for Connection users. This chapter summarizes the Connection conversation and the ways that you can customize it.

See the following sections:

- [How Outside Callers Interact With Cisco Unity Connection by Phone, page 13-1](#)
- [How Users Interact With Cisco Unity Connection by Phone, page 13-1](#)
- [How Administrators Can Customize the User Conversation, page 13-2](#)
- [How Users Can Customize the User Conversation, page 13-5](#)

How Outside Callers Interact With Cisco Unity Connection 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 Connection automated attendant, conduct user searches by using directory assistance, use call routing options, and play audiotext messages.

How Users Interact With Cisco Unity Connection by Phone

When users log on to Cisco Unity Connection by phone, they hear the user conversation. Its collection of prompts enables users to log on to Connection, enroll as new Connection users, send and receive messages, record greetings, and change their personal settings.

There are two ways in which users can interact with 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 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 log on to Connection.

How Administrators Can Customize the User Conversation

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 13-2](#)
- [Customizing the Language of System Prompts, page 13-2](#)
- [Class of Service Settings, page 13-2](#)
- [User Account and Template Settings, page 13-3](#)
- [Using the Custom Keypad Mapping Tool, page 13-4](#)

Advanced Conversation Configuration Settings

From the Advanced Conversation Configuration page in Connection Administration, some of the systemwide conversation customizations that you can make for all users include:

- Changing the order in which 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](#)” chapter for information and procedures for customizing the Connection conversation from the Advanced Conversation Configuration page.

For information on all available advanced conversation configuration settings, see the “[Conversation Configuration](#)” section in the “Advanced Settings” chapter of the *Interface Reference Guide for Cisco Unity Connection Administration*.

Customizing the Language of System Prompts

Revised May 2009

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 Connection users and callers. For steps on changing the default language that Connection uses to play system prompts, see the “[Language of System Prompts](#)” section on page 14-6.

Note that all system prompts are automatically deleted and replaced when you upgrade 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 email in a 3rd-party message store.
- 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”](#) chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

User Account and Template Settings

Revised May 2009

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 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 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 Connection asks a user for a password if the user is calling from the primary extension or an alternate extension.
- Specifying how long Connection waits for a user to respond to a menu, and how many times 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. Although users can use phone keypad keys instead of voice commands at any time, you cannot specify the phone keypad conversation that is offered with the voice-recognition conversation.
- Selecting the actions that Connection performs when the user calls 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 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 Connection performs when messages are played, including announcing the name and number of the sender who left a message, and whether the timestamp 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 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 Connection prompts to confirm message recipients by name.
- Specifying that Connection prompts to continue adding names after each recipient.
- Specifying that 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”](#) chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Using the Custom Keypad Mapping Tool

Revised May 2009

The Custom Keypad Mapping tool allows you to edit the key mappings that are associated with the three Custom Keypad Mapping conversations. Within each of these three 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 Connection Administration.

For more information and procedures, see the [“Custom Keypad Mapping Tool”](#) chapter.

How Users Can Customize the User Conversation

Revised May 2009

Cisco Unity Connection users can customize the conversation that they hear in a number of ways. See [Table 13-1](#) for a summary.

Table 13-1 *Settings That Users Can Change By Using the Cisco Unity Assistant and the Phone Menus*

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Call Holding and Screening ¹ : <ul style="list-style-type: none"> • Select how 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 • Select how Connection handles indirect calls, including telling the user who the call is for, announcing that 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 : <ul style="list-style-type: none"> • None
Call Transfers ² : <ul style="list-style-type: none"> • Configure the three basic transfer rules: standard, alternate, and closed hours • Enable or disable personal call transfer rules for each of the basic transfer rules • Transfer indirect calls to an extension or send them to the user greeting • Change extensions 	Call Transfers ² : <ul style="list-style-type: none"> • Configure the three basic transfer rules: standard, alternate, and closed hours • Enable or disable personal call transfer rules for each of the basic transfer rules • Transfer indirect calls to an extension or send them to the user greeting • Change extensions • Configure alternate contact numbers for caller input keys that are assigned to the Transfer to Alternate Contact Number action
Caller Options: <ul style="list-style-type: none"> • Allow callers to edit messages • Allow callers to mark messages urgent 	Caller Options: <ul style="list-style-type: none"> • None

Table 13-1 Settings That Users Can Change By Using the Cisco Unity Assistant and the Phone Menus (continued)

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Phone Menu Options: <ul style="list-style-type: none"> • Set language for Connection prompts • Specify whether users use the phone keypad or voice-recognition input style • Set speed and volume of prompts, recorded names, and user greetings • Select full or brief Connection conversation menus • Select the action that Connection performs when the user calls Connection, including greeting the user by name, and announcing the number of new messages by type • Specify alternate extensions 	Phone Menu Options: <ul style="list-style-type: none"> • Select full or brief Connection conversation menus
Greetings: <ul style="list-style-type: none"> • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting • Switch between system prompt and personal greeting 	Greetings: <ul style="list-style-type: none"> • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting
Message Notification: <ul style="list-style-type: none"> • Enable or disable a notification device • Specify dialing or recipient options • Select the types of messages and message urgency for which Connection generates a notification • Specify a list of message senders (by user name or calling phone number) for which Connection generates a notification • Set up a notification schedule, and specify what happens when a device does not answer, is busy, or fails 	Message Notification: <ul style="list-style-type: none"> • Enable or disable a notification device, and change its number

Table 13-1 *Settings That Users Can Change By Using the Cisco Unity Assistant and the Phone Menus (continued)*

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
<p>Message Playback:</p> <ul style="list-style-type: none"> Specify the speed and volume of messages that are played by phone Specify message playback order Change the time format used for message time stamps Specify whether Connection plays the Message Type menu Select the action that Connection performs when messages are played, including announcing the name and number of the sender who left a message, and whether the timestamp is played before or after the message Specify that messages are marked saved upon hang-up or disconnect Specify whether Connection asks to confirm deletions of new and saved messages 	<p>Message Playback:</p> <ul style="list-style-type: none"> Speed and volume of message as it is played
<p>Message Sending and Addressing:</p> <ul style="list-style-type: none"> Specify that Connection prompts to confirm message recipients by name Specify that Connection prompts to continue adding names after each recipient Specify that Connection sends messages when users hang up or a call is disconnected Switch between addressing messages to other users by name, or by extension Specify order for addressing messages by name (last name then first name, or vice versa) 	<p>Message Addressing:</p> <ul style="list-style-type: none"> Switch between addressing to other users by name or by extension (by pressing ##)³ Review, add, or remove names in the addressing priority list⁴
<p>Personal Settings:</p> <ul style="list-style-type: none"> Record a name Specify alternate names Change directory listing status Change password 	<p>Personal Settings:</p> <ul style="list-style-type: none"> Record a name Change directory listing status Change password 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
<p>Private Lists:</p> <ul style="list-style-type: none"> Enter a display name Record a list name Add and delete members 	<p>Private Lists:</p> <ul style="list-style-type: none"> Record a list name Add and delete members

Table 13-1 *Settings That Users Can Change By Using the Cisco Unity Assistant and the Phone Menus (continued)*

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Personal Contacts: <ul style="list-style-type: none"> Set up an address book of personal contacts to use for both name dialing and call transfer rules 	Personal Contacts: <ul style="list-style-type: none"> None
<ol style="list-style-type: none"> 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. 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. Note that this depends on whether you have enabled spelled name addressing. 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. 	



CHAPTER 14

Changing Conversation Settings for All Users

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 Password Entry Conversation, page 14-1](#)
- [Addressing Priority Lists, page 14-2](#)
- [Addressing and Recording Order, page 14-3](#)
- [Call Waiting Hold Time, page 14-3](#)
- [Caller Information, page 14-4](#)
- [Dial Prefix Settings for Live Reply to Unidentified Callers, page 14-5](#)
- [Deleting Messages, page 14-5](#)
- [Language of System Prompts, page 14-6](#)
- [Logging On to Cisco Unity Connection from a User Greeting, page 14-7](#)
- [Requesting Users Re-Enter Only the Password After a Failed Password Entry, page 14-8](#)
- [Saving Speed and Volume Changes Made by Users, page 14-9](#)
- [Skipping Messages: Saving New Messages, page 14-9](#)
- [Voice Recognition: Allowing Users to Say Their Voice Mail Passwords, page 14-10](#)
- [Voice Recognition: Confirmation Confidence Threshold, page 14-11](#)
- [Voice Recognition: Global Nickname List, page 14-12](#)
- [Additional Advanced Conversation Configuration Settings, page 14-13](#)

Accessibility Settings in Effect During the Password Entry Conversation

By default, individual user phone menu accessibility settings do not take effect until after the user is authenticated by entering the voice mail password. You can configure Cisco Unity Connection to apply individual user accessibility settings during the password 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 Password Entry Conversation”](#) procedure.

When enabled, the following accessibility settings are applied during the password 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 Passwords

To Enable Accessibility Settings During the Password Entry Conversation

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **Conversations**.
- Step 2** On the Conversation Configuration page, check the **Apply User Accessibility Settings for Voice Mail Password Entry Conversation** check box.
- Step 3** Click **Save**.
-

Addressing Priority Lists

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 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 click **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** Click **Save**.
-

Addressing and Recording Order

The Cisco Unity Connection standard conversation can be customized to change the order in which 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, 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 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 Connection prompts users to address and record when they reply to messages; 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 click **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, 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, Connection prompts them to record the message first and then address it. (This is the default setting.)
- Step 3** Click **Save**.
-

Call Waiting Hold Time

With call holding, when the phone is busy, Cisco Unity Connection can ask callers to hold. 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, 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).

To Add or Change Call Holding Wait Time

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **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 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 Connection from functioning as designed. (The default setting is 5 seconds.)
- Step 4** Click **Save**.

Caller Information

Revised May 2009

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 14-1](#).

Table 14-1 *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, Connection uses Text to Speech to play the display name. If the user does not have a display name, Connection plays the primary extension instead.	Both the recorded name (if available) and the primary extension (if available) before playing the message. If the user (or call handler) does not have a recorded name, 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 Connection users with additional caller information before message playback, consider the following requirements:

- Users hear sender information before Connection plays each message only if their accounts are configured to play it. Either a Connection administrator or a user can specify message playback preferences. (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 Cisco Unity Assistant.)
- In addition, to allow Connection to provide the phone number (ANI or caller ID) information for outside callers, your phone system must support sending such information to Connection. (See your phone system documentation for more information.) When 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” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Dial Prefix Settings for Live Reply to Unidentified Callers

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 Connection users, or if they can return calls to messages from both users and unidentified callers (outside callers or users who are forwarded to Connection but who cannot be identified by the calling extension).

When a user attempts to reply by calling an unidentified caller, 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, Connection returns the call by performing a release transfer to the ANI.

To configure a prefix that 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 click 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 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 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 Connection never prepends digits when performing live reply to unidentified callers. (The default setting is 0 digits.) |
| Step 4 | Click Save . |
-

Deleting Messages

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, 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 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; Connection prompts them: “To delete only your voice messages, press 1. To delete all messages, press 2.” (Default setting)

- 2—Connection does not prompt users to choose which messages to delete; instead, Connection deletes all of their deleted voice messages.
- 3—Connection does not prompt users to choose which messages to delete; instead, Connection deletes all of their deleted messages (voice messages, receipts, and email messages, as applicable).
- Enable 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, Connection does not ask them to confirm the deletion.

You can enable 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

Revised May 2009

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 Connection components without changing the default language settings for the rest of the system.

The phone language setting is available for the following 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 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, 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 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, 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 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	Connection users are able to record greetings in each language installed on the 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” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

To Change the Default Language for System Prompts

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **General Configuration**.
- Step 2** On the General Configuration page, in the System Default Language list, click the language that Connection uses as the default language for playing system prompts.
- Step 3** Click **Save**.
- Step 4** Restart the Voice Processing server role for your changes to take effect.

Logging On to Cisco Unity Connection from a User Greeting

Caller input settings allow you to specify how users log on 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 log on to Connection, and what users hear after Connection prompts them to log on.

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, Connection is set up so that users hear the Connection Sign-In conversation, which prompts them for their ID and password 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 log on from their own greeting by offering the Easy Sign-In conversation, which prompts users only for a password.

[Table 14-2](#) summarizes the options available to you for specifying how users log on to Connection from their own greeting or from another user greeting.

Table 14-2 *Summary of Caller Input Options Available for Specifying How Users Log On to Cisco Unity Connection from User Greetings*

Conversation	Description	Use	Best Practice
Sign-In	Prompts users to enter an ID and password when they press * during any user greeting. Enabled by default.	To avoid leaving a message as an unidentified caller, users can log on to Connection from another user greeting when they call the user from a phone that is not associated with their account. (Connection users cannot reply to messages from unidentified callers.)	Continue to offer the Sign-In conversation. 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.
Easy Sign-In	Prompts users to enter a password when they press a key during any user greeting. Disabled by default. (No key is mapped to the Easy Sign-In conversation.)	Users can dial their extensions and log on quickly without having to remember the pilot number to access Connection by phone. Users may prefer Easy Sign-In to the Sign-In conversation because it saves them from having to re-enter an extension during the logon process. Note that Connection uses the calling extension (rather than the dialed extension) to determine which mailbox the user is trying to log on to.	Provide Easy Sign-In to users who want a faster way to log on from their own greeting or to accommodate users who are accustomed to another voice messaging system. 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: <ul style="list-style-type: none"> • Avoid reassigning the * key so that you can continue to offer the Sign-In conversation. • The # key is already set up to skip greetings. It is also the key that users use to skip ahead throughout the Connection conversation. • The 0 key is already set up to send callers to the Operator call handler.

Requesting Users Re-Enter Only the Password After a Failed Password Entry

When users call Cisco Unity Connection from their extensions or alternate extensions, Connection asks only for a password to authenticate the user. By default, if a user enters an incorrect password, Connection asks for both the user ID and password on subsequent attempts to sign in. Alternatively, you can configure Connection to ask for only the user password on subsequent attempts to sign in.

Note that the default behavior has been set for security reasons; asking for only the user password gives hackers confirmation that the user ID was legitimate.

To Configure Cisco Unity Connection to Ask Only for the User Password After a Failed Password Entry

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **Conversations**.
- Step 2** On the Conversation Configuration page, uncheck the **Request Entry of User ID After Failed Password Entry from Known Extension** check box.
- Note that 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** Click **Save**.
-

Saving Speed and Volume Changes Made by Users

Added May 2009

**Note**

The functionality described in this section is applicable only to Cisco Unity Connection Release 7.1(1) and later.

Speed and volume changes that users make while listening to messages or to the Cisco Unity Connection conversation will be saved as new default settings for the user. (Note that the voice-recognition conversation is the only conversation that allows users to change the Connection conversation speed or volume by phone.)

Do the following procedure to specify whether speed and volume changes made by users are saved by 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 click **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 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 Connection conversation are in effect only for the duration of that phone session.
- Step 3** Click **Save**.
-

Skipping Messages: Saving New Messages

Revised May 2009

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, Connection saves the message as new. This means that when users call Connection to check messages, the skipped message remains in the list of new messages that Connection plays. In addition, message waiting indicators (MWI) on user phones remain lit as long as there are new messages.

Alternatively, you can configure 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 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 click **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** Click **Save**.
-

Voice Recognition: Allowing Users to Say Their Voice Mail Passwords

You can customize the Cisco Unity Connection logon process so that voice recognition users can say the digits in their voice mail passwords to log on when calling Connection from their primary or alternate extensions. Connection attempts to match the spoken digits to the user voice mail password 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 logon process.

In order to use the voice mail password 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 Connection Voice Recognizer to be authenticated by 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 password rather than saying the digits, even when this feature is enabled. However, users cannot mix voice and phone keypad keys for password entry—if the user starts to use the keypad to enter the password, voice recognition is disabled until the user logs on successfully. Also, after a single unsuccessful attempt to say the voice mail password, the user must use the keypad to retry the password entry.

To Allow Voice Recognition Users to Say Their Voice Mail Passwords

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **Conversations**.
- Step 2** On the Conversation Configuration page, check or uncheck the **Allow Voice Recognition Users to Speak Their Voice Mail Passwords** check box, depending on how you want to change the setting:
- **Check box checked**—Voice recognition users can enter their voice mail passwords either by saying the digits in the password, or by using the phone keypad. Connection allows users to say their passwords 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 voice mail passwords by using the phone keypad. (This is the default setting.)
- Step 3** Click **Save**.
-

Voice Recognition: Confirmation Confidence Threshold

Revised May 2009

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 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—Connection always prompts for confirmation regardless of the Voice Recognition Confirmation Confidence Threshold setting. Likewise, 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 click **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** Click **Save**.
-

Voice Recognition: Global Nickname List

Revised May 2009

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, 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 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 click **Global Nicknames**.
- Step 2** On the Search Global Nicknames page, click **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** Click **Save**.
- Step 6** If there is more than one nickname, click **Add New**, replace the Must-Be-Unique-Nick-Name text in the new field with the next nickname and click **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 click **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 click **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 click **Delete Selected**.
- Step 4** Click 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 click **Delete Selected**.
- Click **Add New** to add a new nickname, and enter the applicable information.

Step 5 Click **Save**.

Additional Advanced Conversation Configuration Settings

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 “Advanced Settings” chapter of the *Interface Reference Guide for Cisco Unity Connection Administration* (unless otherwise indicated).

- Remote Port Status Monitor settings
- Disable Identified User Messaging Systemwide
- Full Mailbox Check for Outside Caller Messages
- 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
- Skip Recording of Greeting During Enrollment
- Time to Wait Between Spoken Words (in Milliseconds)
- Maximum Call Transfer Attempts Allowed
- 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](#)” section on page 26-6)
- Use Last (Rather than First) Redirecting Number for Routing Incoming Call
- Cross-Server settings



CHAPTER 15

Custom Keypad Mapping Tool

The Custom Keypad Mapping tool allows you to edit the key mappings that are associated with the three Custom Keypad Mapping conversations. Within each of these three 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.

See the following sections for details:

- [Using the Custom Keypad Mapping Tool, page 15-1](#)
- [Conversation Menus That Can Be Customized, page 15-3](#)
- [Documenting Your Keymap, page 15-13](#)

Using the Custom Keypad Mapping Tool

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 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 clicking 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 click **Custom Keypad Mapping**.

- Step 2** On the Search Custom Keypad Mappings page, click the applicable custom keypad mapping conversation.
- Step 3** On the Edit Custom Keypad Mapping page, click 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 15-2.)
- Step 5** Click **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

Revised May 2009

- 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 blank, 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

Revised May 2009

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 click **Custom Keypad Mapping**.
- Step 2** On the Search Custom Keypad Mappings page, click 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 click **Reset**.
- Step 4** When asked to confirm that you want to replace all key mappings with those of the selected conversation before continuing, click **OK**.
-

Conversation Menus That Can Be Customized

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 15-3](#)
- [Message Playback Menu Tabs \(Message Header Tab, Message Body Tab, and Message Footer Tab\), page 15-4](#)
- [After Message Menu Tab, page 15-9](#)
- [Settings Menu Tab, page 15-11](#)
- [Message Settings Menu Tab, page 15-12](#)
- [Personal Settings Menu Tab, page 15-12](#)

Main Menu Tab

Revised May 2009

The Main menu is what users hear immediately after they sign in and hear their message counts (if applicable).

See [Table 15-1](#) for a list of options that can be mapped.

Table 15-1 **Main Menu Tab**

Option	Description
Play New Messages (<i>Connection 7.1</i>)	Takes users to the new (unread) message stack.
Hear New Messages (<i>Connection 7.0</i>)	
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 personal settings.
Find Messages (<i>Connection 7.1</i>)	Takes users to the Message Locator feature where they can search for new messages by the calling number or name of the sender.
Access Message Locator (<i>Connection 7.0</i>)	This option is offered only when the Finding Messages With Message Locator feature is enabled for each user on the Phone Menu page.

Table 15-1 Main Menu Tab (continued)

Option	Description
List Meetings	Lists the time, meeting organizer, and subject for all current and upcoming meetings. For Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express meetings, the user is offered the option to join current meetings.
Play External Messages (<i>Connection 7.1</i>)	Provides the count of messages that are stored on an external message store.
External Email Messages (<i>Connection 7.0</i>)	The user is offered the option to listen to these messages.
Manage Call Handler Greetings (<i>Connection 7.1</i>)	Allows users to access the Greetings Administrator conversation to change greetings for call handlers that have been assigned an extension.
Greetings Administrator (<i>Connection 7.0</i>)	Users who are assigned to the Greetings Administrator role on the Edit Roles page can change the greetings for any system call handler. Users who are not assigned to the Greetings Administrator role can change the greetings only for call handlers that they own.
Call a Number (<i>Connection 7.1</i>)	Allows users to access the User System Transfer conversation and dial any number that is allowed by their transfer restriction table.
System Transfer (<i>Connection 7.0</i>)	
Manage Broadcast Messages (<i>Connection 7.1</i>)	Allows users to access the Broadcast Message Administration conversation.
Broadcast Message Administration (<i>Connection 7.0</i>)	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 (<i>Connection 7.1</i>)	Exits the user mailbox. 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.
Exit (<i>Connection 7.0</i>)	

Message Playback Menu Tabs (Message Header Tab, Message Body Tab, and Message Footer Tab)

Revised May 2009

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 timestamp.

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 timestamp 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 not playing the timestamp after the message; you can exclude it altogether or have the timestamp 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 timestamp after the message the effect is to have no footer to the message.

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 15-2](#) for a list of options that can be mapped.

Table 15-2 Message Playback Menu Tabs

Option	Description
Repeat Message (<i>Connection 7.1</i>)	Jumps to the beginning of the header portion of the message.
Skip to the Message Header (<i>Connection 7.0</i>)	
Save (<i>Connection 7.1</i>)	Skips to the next message and marks the current message as saved.
Skip Message, Mark Saved (<i>Connection 7.0</i>)	
Delete	Deletes the message that is currently being played. 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. (Applicable to <i>Connection version 7.1(1)</i> and later) After the message has finished playing, the last change made to playback speed is saved as the default playback speed for the user. Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback speed are not saved as the new default.

Table 15-2 Message Playback Menu Tabs (continued)

Option	Description
Fast Playback	<p>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.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback speed is saved as the default playback speed for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback speed are not saved as the new default.</p>
Reset Speed to Default	<p>Resets the speed of the message that is currently being played to the default message playback speed setting for the user.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback speed is saved as the default playback speed for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback speed are not saved as the new default.</p>
Change Volume	<p>Cycles the volume of the message that is currently being played through three volume levels: normal, loud, and quiet.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback volume is saved as the default playback volume for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback volume are not saved as the new default.</p>
Reset Volume to Default	<p>Resets the volume of the message that is currently being played to the default message playback volume setting for the user.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback volume is saved as the default playback volume for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback volume are not saved as the new default.</p>

Table 15-2 Message Playback Menu Tabs (continued)

Option	Description
Quieter Playback	<p>Decreases the volume of the message that is currently being played.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback volume is saved as the default playback volume for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback volume are not saved as the new default.</p>
Louder Playback	<p>Increases the volume of the message that is currently being played.</p> <p><i>(Applicable to Connection version 7.1(1) and later)</i> After the message has finished playing, the last change made to playback volume is saved as the default playback volume for the user.</p> <p>Note If the Save Speed and Volume Changes Made by User setting is not enabled on the System Settings > Advanced > Conversation Configuration page, changes to playback volume are not saved as the new default.</p>
Pause/Resume	Pauses playback of the message, or resumes playback when the message is already paused.
Rewind (<i>Connection 7.1</i>)	Jumps backward in the message that is currently being played.
Rewind Message (<i>Connection 7.0</i>)	By default, the message rewinds five seconds. You can adjust the rewind time on the Playback Message Settings page.
Fast-Forward	<p>Jumps forward in the message that is currently being played.</p> <p>By default, the message fast-forwards five seconds. You can adjust the fast-forward time on the Playback Message Settings page.</p>
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 (<i>Connection 7.1</i>)	Skips to the next message in the stack and marks the message as new.
Skip Message, Mark New (<i>Connection 7.0</i>)	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 (<i>Connection 7.1</i>)	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.
Go to Message (<i>Connection 7.0</i>)	For users who have large numbers of messages, this is a useful way to jump ahead or back in the stacks.
	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 15-2 *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 (<i>Connection 7.1</i>) Exit Message Playback (<i>Connection 7.0</i>)	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. 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 (<i>Connection 7.1</i>) Return Call to Sender (<i>Connection 7.0</i>)	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. 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.
Skip to End (<i>Connection 7.1</i>) Skip to the Message Footer (Time Stamp) (<i>Connection 7.0</i>)	Jumps to the beginning of the message footer (the time stamp). When the After Playing Each Message, Play Time the Message Was Sent option is not enabled for the user on the Playback Message Settings page, this option effectively skips to the end of the message and goes directly to the After Message menu.
Replay Message (<i>Connection 7.1</i>) Skip to the Message Body (<i>Connection 7.0</i>)	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 (<i>Connection 7.1</i>) Go to Operator Call Handler (<i>Connection 7.0</i>)	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. 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. Connection plays the “Last message” prompt as an audible cue to the user.

Table 15-2 *Message Playback Menu Tabs (continued)*

Option	Description
Toggle Urgency Flag	Toggles the priority flag on a received message between urgent and normal. Users who want to identify the high-priority messages among all of their received messages may be interested in this functionality. By default, Connection plays messages that are marked urgent first.
Send to Fax Machine for Printing (<i>Connection 7.1</i>) Send to Fax (<i>Connection 7.0</i>)	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. 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

Revised May 2009

The After Message menu plays after the user has listened to a message.

See [Table 15-3](#) for a list of options that can be mapped.

Table 15-3 *After Message Menu Tab*

Option	Description
Repeat Message (<i>Connection 7.1</i>) Replay Message (<i>Connection 7.0</i>)	Plays the message again, starting with the header.
Save (<i>Connection 7.1</i>) Save/Restore as Saved (<i>Connection 7.0</i>)	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. 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. 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.

Table 15-3 After Message Menu Tab (continued)

Option	Description
Save as New (<i>Connection 7.1</i>) Save as New/Restore as New (<i>Connection 7.0</i>)	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.
Rewind (<i>Connection 7.1</i>) Rewind Message (<i>Connection 7.0</i>)	Jumps backward into the message. 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 (<i>Connection 7.1</i>) Send to Fax (<i>Connection 7.0</i>)	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. 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 (<i>Connection 7.1</i>) Exit, Leave Message As Is (<i>Connection 7.0</i>)	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 (<i>Connection 7.1</i>) Go to Operator Call Handler (<i>Connection 7.0</i>)	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 (<i>Connection 7.1</i>) Go to Message (<i>Connection 7.0</i>)	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. 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. Connection plays the “First message” prompt as an audible cue to the user.

Table 15-3 *After Message Menu Tab (continued)*

Option	Description
Go to Last Message	Jumps to the last message of the message stack. 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. Users who want to identify the high-priority messages among all of their received messages may be interested in this functionality. By default, Connection plays messages that are marked urgent first.
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. 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.
Reply to All	Replies to all recipients of the message.

Settings Menu Tab

Revised May 2009

The Settings menu is what users hear when they choose Change Setup Options from the Main menu.

See [Table 15-4](#) for a list of options that can be mapped.

Table 15-4 *Settings Menu Tab*

Option	Description
Greetings	Allows users to modify their greetings.
Message Settings	Takes users to the Message Settings menu.
Personal Settings	Takes users to the Personal Settings menu.
Transfer Settings	Allows users to modify their transfer rules.
Alternate Contact Numbers	Allows users to change their alternate contact phone numbers. 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.

Table 15-4 Settings Menu Tab (continued)

Option	Description
Cancel or Back Up (Connection 7.1)	Exits the Settings menu and goes up a menu level to the Main menu.
Exit (Connection 7.0)	

Message Settings Menu Tab

Revised May 2009

The Message Settings menu is what users hear when they choose Message Settings from the Settings menu.

See [Table 15-5](#) for a list of options that can be mapped.

Table 15-5 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 (Connection 7.1)	Exits the Message Settings menu and goes up a menu level to the Settings menu.
Exit (Connection 7.0)	

Personal Settings Menu Tab

Revised May 2009

The Personal Settings menu is what users hear when they choose Personal Settings from the Settings menu.

See [Table 15-6](#) for a list of options that can be mapped.

Table 15-6 Personal Settings Menu Tab

Option	Description
Change Phone Password (Connection 7.1)	Allows users to modify their phone passwords.
Password (Connection 7.0)	This option is not available for a user when the User Cannot Change check box is checked on the user Edit Password Settings page.

Table 15-6 **Personal Settings Menu Tab (continued)**

Option	Description
Change Recorded Name (<i>Connection 7.1</i>)	Allows users to record voice names.
Recorded Name (<i>Connection 7.0</i>)	This option is available only when the user is assigned to a class of service that has enabled the Allow Recording of Voice Name option.
Change Directory Listing (<i>Connection 7.1</i>)	Allows users to choose whether or not they want to be listed in the directory.
Directory Listing (<i>Connection 7.0</i>)	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.
Repeat Menu	Plays the Personal Settings menu again.
Help	Plays the Personal Settings menu Help.
Cancel or Back Up (<i>Connection 7.1</i>)	Exits the Personal Settings menu and goes up a menu level to the Settings menu.
Exit (<i>Connection 7.0</i>)	

Documenting Your Keymap

Added May 2009

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”](#) section on page 3-10.



CHAPTER 16

Changing the Audio Format of Recordings and Media Streams

See the following sections:

- [Changing the Audio Format That Cisco Unity Connection Uses for Calls, page 16-1](#)
- [Changing the Audio Format for Recordings, page 16-2](#)

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:

- When Connection advertises a different audio format than the one used by the phone system, the phone system transcodes the media stream.
- 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 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 Servers”](#) chapter of the *Design Guide for Cisco Unity Connection Release 7.x*.

To Change the Audio Format That Cisco Unity Connection Uses for Calls

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.
- Step 2** On the Search Port Groups page, click 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, click **Codec Advertising**.
- Step 4** On the Edit Codec Advertising page, click 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, 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** Click **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, click the applicable packet setting for each codec in the Packet Size list, and click **Save**.
- Step 7** On the Port Group menu, click **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

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, Connection should record messages in the same audio format that the phone system uses. If users listen to messages on Personal Digital Assistants (PDAs), however, 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 by Connection for recording and playing recorded messages, greetings, and names reduces transcoding between audio formats that Connection must perform, and thus reduces the effect on the performance of the 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 Servers”](#) chapter of the *Design Guide for Cisco Unity Connection Release 7.x*.

To Change the Audio Format for Recording Messages

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **General Configuration**.
- Step 2** On the Edit General Configuration page, in the Recording Format list, click the applicable setting.

**Note**

If the playback device uses a different audio format, 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 Click **Save**.



CHAPTER 17

Managing Recorded Greetings and Recorded Names

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 Cisco Unity Assistant web tool. For end-user instructions and information about using the Media Master, see the *User Guide for the Cisco Unity Connection Assistant Web Tool*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/user/guide/assistant/7xcucugasstx.html.

See the following sections for details:

- [Using the Media Master to Record Greetings and Names, page 17-1](#)
- [Using the Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings, page 17-2](#)
- [Setting Up the Cisco Unity Greetings Administrator, page 17-4](#)
- [Changing the Audio Format for Recording Greetings and Names, page 17-5](#)

Using the Media Master to Record Greetings and Names

Revised May 2009

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 clicking 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, 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 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, click **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.
- Step 5** Click **OK**.
-

Using the 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 or system distribution list.

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 Connection from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.

When a system distribution list owns a call handler, the Cisco Unity Greetings Administrator allows each member of the system distribution list to manage call handler greetings by using the Cisco Unity Connection phone conversation.

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, 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 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 Connection system, at the prompt, press the number of the language in which to edit greetings for the call handler. (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 Cisco Unity Greetings Administrator

Revised May 2009

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 17-4. (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 17-4.
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 17-5.
4. As needed, tell call handler owners how to use the Cisco Unity Greetings Administrator. For an overview and procedure, see the [“Using the Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings”](#) section on page 17-2.

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 click System Call Handlers . |
| Step 2 | On the Search Call Handler page, in the Search Results table, click the Opening Greeting call handler. |
| Step 3 | On the Edit Call Handler Basics page, on the Edit menu, click Caller Input . |
| Step 4 | On the Caller Input page, in the Caller Input Keys table, click 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 choose 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 | Click Conversation , and then click Greetings Administrator in the list. |
| Step 7 | Click 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 click Direct Routing Rules . |
| Step 2 | On the Direct Routing Rules page, click Add New . |
| Step 3 | On the New Direct Routing Rule page, enter a display name for the new routing rule, and click 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, click **Add New**.
- Step 6** On the New Direct Routing Rule Condition page, click **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** Click **Save**.
- Step 8** On the Edit menu, click **Edit Direct Routing Rule**.
- Step 9** On the Edit Direct Routing Rule page, in the Send Call To field, click **Conversation**, then click **Greetings Administrator**.
- Step 10** Click **Save**.
- Step 11** On the Direct Routing Rule menu, click **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** Click **Change Order**.
- Step 13** On the Edit Direct Routing Rule Order page, click the name of the rule that you want to reorder, and click the Up or Down arrow until the rules appear in the correct order.
- Step 14** Click **Save**.
-

To Assign a Unique Extension to a Call Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **System Call Handlers**.
- Step 2** On the Search Call Handlers page, in the System Call Handlers table, click 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** Click **Save**.
-

Changing the Audio Format for Recording Greetings and Names

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, 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 Connection must perform, and reduces the effect on the performance of the 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 Mu-Law audio format. However, sound quality is preserved when greetings 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 Greetings and Names

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then click **General Configuration**.

Step 2 On the Edit General Configuration page, in the Recording Format list, click the applicable setting. Connection records all messages, greetings, and names in the audio format that you select.



Note If the playback device uses a different audio format, 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 Click **Save**.



CHAPTER 18

Specifying Password, Logon, and Lockout Policies

See the applicable sections, depending on your configuration:

- [Cisco Unified Communications Manager Business Edition \(CMBE\) Only, page 18-1](#)
- [Cisco Unity Connection Only, page 18-1](#)

Cisco Unified Communications Manager Business Edition (CMBE) Only

In Cisco Unified Communications Manager Business Edition (CMBE), you use Cisco Unified Communications Manager Administration to specify password and account lockout policies for phone and web-tool access, and to specify the logon policy for web-tool access for all users who access Cisco Unity Connection voice messages.

The policies are specified on the User Management > Credential pages in Cisco Unified CM Administration. See the online Help, or the *Cisco Unified Communications Manager Administration Guide* for details and related topics. (Administration documentation for Cisco Unified Communications Manager is available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.)

Note that although you cannot set password, logon, and lockout policies in Cisco Unity Connection Administration, you can change a Connection user password on the user account page. See the “[Passwords](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*. Alternatively, users can change their own passwords in the Cisco Unity Assistant.

Cisco Unity Connection Only

In Cisco Unity Connection, you use authentication rules to determine the password and account lockout policies for phone and web-tool access, and to specify the logon policy for web-tool access for all users who access Cisco Unity Connection voice messages.

See the following sections:

- [Specifying Password, Logon, and Lockout Policies by Using Authentication Rules \(Cisco Unity Connection Only\), page 18-2](#)

- [Creating and Modifying Authentication Rules, and Assigning Rules to Users \(Cisco Unity Connection Only\)](#), page 18-2

Specifying Password, Logon, and Lockout Policies by Using Authentication Rules (Cisco Unity Connection Only)

In Cisco Unity Connection, authentication rules govern user passwords and account lockouts for all user accounts. You use authentication rules to secure how users access 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 logon 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
- The number of days before a password expires

Creating and Modifying Authentication Rules, and Assigning Rules to Users (Cisco Unity Connection Only)

Authentication rules are specified on the System Settings > Authentication Rules page in Cisco Unity Connection Administration. Connection includes the following predefined authentication rules:

Recommended Voice Mail Authentication Rule	By default, Connection applies this rule to the Voice Mail password on the Password Settings page of each user account and user template for which you set up user access to Connection by phone.
Recommended Web Application Authentication Rule	By default, 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 Connection. For information on specifying an authentication rule for a user account or template, see the “[Passwords](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.



CHAPTER 19

Messaging

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 Connection, and discusses how Connection handles the recording, delivery, and storage of messages.

See the following sections:

- [Types of Messages, page 19-1](#)
- [Message Recording, page 19-4](#)
- [Default Recipient Accounts, page 19-5](#)
- [Dispatch Messages, page 19-6](#)
- [Message Delivery, page 19-9](#)
- [Message Delivery and Sensitivity Options, page 19-12](#)
- [Message Actions, page 19-13](#)
- [Message Subject Line Formats, page 19-13](#)
- [Message Storage, page 19-17](#)
- [Message Access, page 19-17](#)
- [Configuring Live Record, page 19-18](#)
- [Configuring Access to RSS Feeds of Voice Messages, page 19-20](#)

Types of Messages

Revised May 2009

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 logged into Connection—can reach user mailboxes to leave messages in a number of different ways, depending on the Connection configuration. A caller can call the main phone number for the 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 Connection when the user does not answer, and then leave a message.

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 Cisco Unity 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 log in, then send a message to one or more other Connection users or to a distribution list. Connection identifies the sender of the message as a user; when the called user later listens to the message, Connection plays the recorded voice name of the user (or displays the user name when the called user views the message in a Cisco web application such as the Cisco Unity Inbox, or from an IMAP client).

Alternatively, a user can call the extension of another user and be forwarded to 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, 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 an External Message Store

By using the IMAP protocol, 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 log on 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 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](#)” chapter for more information on setting up and using system broadcast messages.

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 cell phones. When a message arrives that matches the criteria selected in the message notification settings, the Connection Messaging System sends a text message entered by you or the user, such as “Urgent message for Technical Support.” Connection can also dial a phone number to alert the user of a new message and allow the user to enter credentials to log in and listen to the message.

By default, if Connection sends a notification of a new message to a device (such as a cell phone) and the device forwards the call back to Connection because the device did not answer, Connection rejects the forwarded message notification call. As a result, the user mailbox is not filled with forwarded message notification announcements. Because 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](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* for more information on setting up various types of notifications.

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 activate 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](#)” 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](#)” section on page 19-6 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” section on page 19-18](#) for information on configuring live record.

Message Recording

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, 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, 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 Connection must perform, and reduces the effect on the performance of the 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 click **General Configuration**.

Step 2 On the Edit General Configuration page, in the Recording Format list, click the applicable setting.



Note If the playback device uses a different audio format, 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 Click **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 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 click **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 Connection monitors the recording length to determine whether to play a termination warning prompt.

Note that recordings that are not allowed to exceed this length are not monitored by 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 Connection plays a termination warning prompt. When the warning is played during a recording session, Connection continues recording for the amount of time indicated in this field before terminating the recording session.
- Step 4** Click **Save**.

Default Recipient Accounts

Revised May 2009

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 voice mail and web application passwords. To log on 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 voice mail and web application passwords. To log on to the account, you must change the passwords by using Cisco Unity Connection Administration.

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 Connection Messaging System mailbox (UnityConnection@<servername>).

The alias for this account is UnityConnection. This account can be viewed in Cisco Unity Connection Administration, but cannot be modified or deleted.

Dispatch Messages

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 19-7](#)
- [To Configure Dispatch Messaging for Messages Left for an Interview Handler, page 19-7](#)

Also see the “[Dispatch Messaging Limitations and Behavioral Notes](#)” section on page 19-7.

To Configure Dispatch Messaging for Messages Left for a Call Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **System Call Handlers**.
- Step 2** On the Search Call Handlers page, in the System Call Handlers table, click the display name of the applicable call handler.
- Step 3** On the Edit Call Handler Basics page, on the Edit menu, click **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** Click **Save**.
-

To Configure Dispatch Messaging for Messages Left for an Interview Handler

- Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then click **Interview Handlers**.
- Step 2** On the Search Interview Handlers page, in the Interview Handlers table, click 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** Click **Save**.
-

Dispatch Messaging Limitations and Behavioral Notes

Revised May 2009

- 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 Cisco Unity Inbox, Cisco Unified Personal Communicator, 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” section on page 19-13.](#)) 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 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 either the Cisco Unity 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, Connection interprets that key press as “postpone” or “decline” respectively.
- 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 voice mail 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 voice mail 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.
- Dispatch messaging is not supported with digital networking. If remote users are members of a distribution list that is the recipient of a call handler that is configured to mark messages for dispatch delivery, those remote users receive the message as a normal voice message. They are not offered the option to accept, postpone, or decline the message.
- If 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 most cases, Cisco Unity Connection delivers messages from callers by using a standard process—Connection logs on to the sender account (either the 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 19-9](#)
- [How Cisco Unity Connection Handles Messages When System Components Are Unavailable, page 19-9](#)
- [How Cisco Unity Connection Handles Messages That Are Interrupted by Disconnected Calls, page 19-10](#)
- [How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded, page 19-11](#)
- [How Cisco Unity Connection Handles Messages When Maximum Mailbox Store Size Is Exceeded, page 19-11](#)

How Cisco Unity Connection Handles Messages That Cannot Be Delivered

Revised May 2009

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 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, 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), Connection queues any messages that are recorded by users or outside callers, and delivers them when the component becomes available.

External Server Is Unavailable

If Connection is configured to allow users access to email messages in an external message store, and network or other conditions slow or prevent responses when Connection attempts to retrieve messages from Exchange, Connection announces to users that email is unavailable when they attempt to access email messages. The time period that Connection waits for a response from the external message store defaults to four seconds, and is configurable in Cisco Unity Connection Administration. Do the following procedure to change the length of the timeout.

To Change the Timeout Period That Cisco Unity Connection Waits for an External Service Response

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **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** Click **Save**.
The change takes effect immediately.
-

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

Revised May 2009

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 cell phone loses its charge or signal.

By default, 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 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 Connection sends the message even though the user may not have recorded an introduction or completely addressed the message.

You can configure 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 #, 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” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded

Revised May 2009

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, 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 logs on to Connection and attempts to send a message to another user, 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, Connection sends a nondelivery receipt to the message sender.

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, Connection logs an error. (The warning and error messages can be viewed in the Real-Time Monitoring Tool.) However, Connection functionality is not affected. You can continue to add or move mailboxes to a mailbox store that has reached the maximum size, and 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](#)” chapter.

Message Delivery and Sensitivity Options

Revised May 2009

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.

Connection offers the following message delivery and sensitivity options for users and outside callers:

Urgent	<p>Urgent messages are delivered before normal messages.</p> <p>Users who are logged on to their mailboxes can always mark a message urgent. When unidentified callers and users who have not explicitly logged on 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.</p>
Private	<p>Private messages can be sent to anyone, but the message cannot be forwarded or saved locally as a WAV file by a recipient listening to it by phone or from the Cisco Unity Inbox. Recipients who listen to a private message via an IMAP client can forward the message, and can save it. (See the “Message Security Options for IMAP Client Access” section on page 24-3 to learn how to prevent this.)</p> <p>User-to-user messages can be marked private. Outside callers and users who have not explicitly logged on to their mailboxes cannot mark a message private.</p>
Secure	<p>Only Connection users can receive a secure message. The message can be played and forwarded by phone and from the Cisco Unity Inbox and from Cisco Unity Connection ViewMail for Microsoft Outlook and from Cisco Unity Connection ViewMail for IBM Lotus Notes, but it cannot be accessed from an IMAP client other than Microsoft Outlook or Lotus Notes with ViewMail. The message cannot be saved locally as a WAV file.</p> <p>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 logged on to their mailboxes cannot mark a message secure. Instead, the Mark Messages Secure check box on the Edit > Message Settings page for a user account or call handler determines whether Connection automatically marks messages from outside callers secure, or delivers them with normal sensitivity.</p> <p>Note In Cisco Unity Connection 7.0, the field name is “Mark Secure.”</p>
Future Delivery	<p>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 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.</p> <p>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.</p>

The [“How Cisco Unity Connection Handles Messages That Are Marked Private or Secure”](#) section on page 24-1 details how Connection handles private and secure messages.

Message Actions

Revised May 2010

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 Connection server from any client (for example, by using the phone interface, the Cisco Unity Assistant, or an IMAP client).

By default, Connection is configured to accept each type of message, an action that causes Connection to place the message in the user mailbox in the applicable Connection mailbox store.

You can use the relay action to instruct 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 Connection phone interface, from the Cisco Unity 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 Connection is configured to connect so that users can hear their emails read to them when they log on to 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 the Bulk Edit utility; in these cases, you can use a combination of text and replaceable tokens to define a template for the SMTP address, from which Connection creates a relay address for each individual user.) Note that Connection relays messages through an SMTP smart host, and you must have the smart host configured on the Connection server before you can configure this action for a user or user template.

In Cisco Unity Connection 7.1, you can use the accept and relay action to instruct 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 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 Connection message store. Note that if the user does not regularly manage new messages in the 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 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

Message subject lines are visible when users view and listen to messages in the Cisco Unity 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 Connection users who send messages without first logging on to Connection or who have not been automatically identified as 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 logged on to Connection, or have been automatically identified as 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 19-14](#)
- [Subject Line Format Examples, page 19-16](#)
- [Subject Line Format Configuration, page 19-16](#)

Subject Line Parameters

Revised May 2009

[Table 19-1](#) describes the parameters that can be used to define message subject lines.

Table 19-1 *Parameters Used to Define Message Subject Lines*

Parameter	Description
%CALLERID%	<p>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.</p> <p>If the ANI Caller ID is not available, the text entered in the %CALLERID% (When Unknown) field is inserted into the subject line instead.</p>
%CALLEDID%	<p>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.</p> <p>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.</p>

Table 19-1 *Parameters Used to Define Message Subject Lines (continued)*

Parameter	Description
%NAME%	<p>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.</p> <p>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, Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field.</p> <p>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, Connection inserts the display name of the interview handler. If the display name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field.</p> <p>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, Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field.</p>
%EXTENSION%	<p>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.</p> <p>If the extension is not available, the value entered in the %EXTENSION% (When Unknown) field is inserted into the subject line instead.</p> <p>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.</p>
%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 19-2 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

Revised May 2009

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 19-1](#).
 - Step 4** Enter text in the Parameter Definitions fields, as applicable.

Step 5 Click **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

Revised May 2009

Cisco Unity Connection stores message content as files on the Connection server, and stores information about the messages in a database.

Depending on the number of 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 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 Connection users nor outside callers are allowed to leave voice messages. 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 Connection Message Transfer Agent service.

If the hard disk exceeds the value that you specify, instruct 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”](#) chapter.

**Note**

For ways to prevent users from saving messages as WAV files to their hard drives or other locations outside of the Connection server, see the [“Securing User Messages: Controlling Access and Distribution”](#) chapter.

Message Access

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 Inbox, the Cisco Personal Communicator, or an RSS reader. When set up to do so, users can access Connection voice messages from an IMAP client, Cisco Unified Messaging with IBM Lotus Sametime, or an RSS reader.

Finally, depending on their external service accounts, users may access email messages in an external message store by phone.

Configuring Live Record

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, click **Directory Number**.
 - Step 2** On the Find and List Directory Numbers page, click **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, click the partition that contains all voice mail 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, click 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 voice mail pilot number for the Cisco Unity Connection voice messaging ports.
 - Step 9** In the Forward All field, under Calling Search Space, click the calling search space that includes the partition that you selected in [Step 4](#).
 - Step 10** Click **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, click **Service Parameters**.
 - Step 2** On the Service Parameters Configuration page, in the Server field, click the name of the Cisco Unified CM server.
 - Step 3** In the Service list, click **Cisco CallManager**. The list of parameters appears.
 - Step 4** Under Clusterwide Parameters (Feature - Conference), in the Drop Ad Hoc Conference field, click **When Conference Controller Leaves**.

- Step 5** Click **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 click **Call Routing > Forwarded Routing Rules**.
- Step 2** On the Forwarded Routing Rules page, click **Add New**.
- Step 3** On the New Forwarded Routing Rule page, in the Description field, enter **Live Record** or another descriptive name and click **Save**.
- Step 4** On the Edit Forwarded Routing Rule page, in the Status field, click **Active**.
- Step 5** Under Send Call To, click **Conversation**.
- Step 6** In the Conversation list, click **Start Live Record**.
- Step 7** Click **Save**.
- Step 8** Under Routing Rule Condition, click **Add New**.
- Step 9** On the New Forwarded Routing Rule Condition page, click **Dialed Number**.
- Step 10** To the right of the Dialed Number option, click **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 19-18](#). For example, enter “5110.”
- Step 11** Click **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 click **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** Click **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 19-18](#). For example, dial “5110.”

- Step 4** To join the 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, log on to the voice mailbox for the user.
- Step 7** Listen to the recorded phone conversation.
-

Configuring Access to RSS Feeds of Voice Messages

As an alternative to checking messages by phone or using the Cisco Unity 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 Cisco Unity Inbox and RSS Feeds, and the Connection Inbox RSS Feed service must be activated and started. Do the following procedure.

To Confirm That the Inbox RSS Feed Service Is Activated and Started

- Step 1** In Cisco Unity Connection Serviceability, click **Tools > Service Management**.
- Step 2** In the Optional Services section, confirm that the Connection Inbox RSS Feed service is activated and started.
-

See the following sections for additional details on configuring access to RSS Feeds:

- [Allowing Insecure Connections to RSS Feeds, page 19-20](#)
- [Configuring an RSS Reader to View Voice Messages, page 19-21](#)
- [RSS Feed Limitations and Behavioral Notes, page 19-21](#)

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 that 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** Click **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://<Connection server name>/cisco-unity-rss/rss.do`
- 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.

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.



CHAPTER 20

Configuring IMAP Settings

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 Connection server.

See the following sections:

- [SMTP Message Handling Overview, page 20-1](#)
- [Integrated Messaging Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook, page 20-2](#)
- [Recommendations for Deploying IMAP Access, page 20-3](#)
- [Task List for Configuring IMAP Access in Cisco Unity Connection, page 20-3](#)
- [Procedures for Configuring IMAP Access in Cisco Unity Connection, page 20-4](#)

SMTP Message Handling Overview

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 Connection through SMTP, Connection attempts to categorize the message as a voice mail, email, fax, or delivery receipt. 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 Connection user, Connection processes the message for each individual recipient based on the type of recipient:

- If the recipient maps to a VPIM contact, Connection converts the message into a VPIM message, removing any attachment that is not allowed by the VPIM standard. Then, 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 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, 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

Connection accepts the message and places it in the user mailbox on the 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 Connection server, 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, 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, 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 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, Connection puts the message into the MTA bad mail folder (UmssMtaBadMail).

Note that 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 Handles Messages That Are Marked Private or Secure”](#) section on page 24-1 for more information about who can receive and access secure messages.

Integrated Messaging Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook

Added May 2009

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 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 clicks on 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 clicks the Send button. In this case, because ViewMail is configured to use the Connection IMAP account to send messages, the voice message is routed to the Connection server for delivery.

When 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, 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 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 that because Connection is configured to be able to match the corporate email addresses in use at ExampleCo to 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

Revised May 2009

When deploying IMAP clients to access and send Cisco Unity Connection messages, we recommend the following:

- Use a firewall to protect the 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 Connection IMAP account on user workstations, use the corporate email address of the user, rather than the 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 Connection-specific addresses if the 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

Revised May 2009

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 Connection server. See the documentation for the SMTP server application that you are using.
 - b. Configure the 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 20-4.
 - c. *In Cisco Unity Connection 7.1 only:* Review the settings that control whether private or secure messages can be relayed. See the [“Configuring Message Relay Settings \(Cisco Unity Connection 7.1 and Later\)”](#) section on page 20-5.
2. Configure message actions for Connection users or user templates. See the [“Message Actions”](#) section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

3. Configure SMTP proxy addresses for users who will send or receive messages from IMAP clients. See the [“SMTP Proxy Addresses”](#) section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.



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”](#) section in the “Setting Up Features and Functionality That Are Controlled by Class of Service” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
5. Configure SMTP proxy addresses for VPIM contacts who may receive messages from IMAP clients. See the [“SMTP Proxy Addresses”](#) section in the “Managing Contacts” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
6. Configure the 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 20-5.
7. *If you configured Transport Layer Security to be required or optional in the procedure in Task 6.:* Configure the Connection server to provide a secure IMAP connection, as described in the [“Creating and Installing an SSL Server Certificate”](#) section on page 25-2.
8. Optionally, modify the settings that determine the characteristics of SMTP messages that Connection accepts. See the [“Configuring SMTP Message Parameters”](#) section on page 20-7.
9. For each user workstation, configure a supported IMAP client to access a Connection mailbox. See the [“Configuring an Email Account to Access Cisco Unity Connection Voice Messages”](#) chapter of the *User Workstation Setup Guide for Cisco Unity Connection*.

Procedures for Configuring IMAP Access in Cisco Unity Connection

See the following sections:

- [Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host, page 20-4](#)
- [Configuring Message Relay Settings \(Cisco Unity Connection 7.1 and Later\), page 20-5](#)
- [Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication, page 20-5](#)
- [Configuring SMTP Message Parameters, page 20-7](#)

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 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 click **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** Click **Save**.
-

Configuring Message Relay Settings (Cisco Unity Connection 7.1 and Later)

Added May 2009

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 click **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.) Connection sets the private flag on the message when relaying a private message.
- To prevent Connection from relaying private messages, uncheck the check box. 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 Connection relay secure messages, check the **Allow Relaying of Secure Messages** check box. (This check box is unchecked by default.) Connection relays secure messages as regular messages.
- To prevent Connection from relaying secure messages, uncheck the check box. 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** Click **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 Connection, users enter their Connection alias and Web Application (Cisco PCA) password in the IMAP client to authenticate. Make sure that users understand that whenever they change their Cisco PCA password in the Cisco Unity 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 Logon Problems](#)” section in the “Configuring an Email Account to Access Cisco Unity Connection Voice Messages” chapter of the *User Workstation Setup Guide for Cisco Unity Connection*.

Do one or both of the following procedures, as applicable.

- [To Configure the Cisco Unity Connection IP Address Access List](#), page 20-6
- [To Configure Access and Authentication for Untrusted IP Addresses](#), page 20-6

To Configure the Cisco Unity Connection IP Address Access List

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then click **Server**.
- Step 2** On the SMTP Server Configuration page, on the Edit menu, click **Search IP Address Access List**.
- Step 3** On the Search IP Address Access List page, click **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** Click **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 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, click **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 click **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 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 Connection handles Transport Layer Security for untrusted IP addresses:
- **Disabled**—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 Connection does not offer it, the 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 Connection server.
 - **Optional**—Clients or servers connecting from untrusted IP addresses can use TLS to initiate SMTP sessions with the 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 Connection server, see the [“Creating and Installing an SSL Server Certificate”](#) section on [page 25-2](#).

Configuring SMTP Message Parameters

Revised May 2009

You can configure 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, 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 click **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** Click **Save**.



CHAPTER 21

Managing Mailbox Stores

See the following sections:

- [How Multiple Mailbox Stores Work, page 21-1](#)
- [Creating a Mailbox Store, page 21-4](#)
- [Moving Mailboxes Between Mailbox Stores, page 21-4](#)
- [Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged, page 21-5](#)
- [Deleting a Mailbox Store, page 21-5](#)
- [Disabling and Re-Enabling a Mailbox Store, page 21-7](#)

How Multiple Mailbox Stores Work

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 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 Connection was installed.

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”](#) section on page 21-4.

See the following sections for additional details:

- [Replication, page 21-2](#)
- [User Templates, page 21-2](#)
- [Maximum Size of a Mailbox Store, page 21-2](#)
- [Backups with Multiple Mailbox Stores, page 21-3](#)

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 choose 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 choose 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](#)” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Maximum Size of a Mailbox Store

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:

- 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](#)” section on page 21-5. 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](#)” 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 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsagx.html.
- For Cisco Unified CMBE, see the *Disaster Recovery System Administration Guide for Cisco Unified CMBE* at http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html.

Creating a Mailbox Store

To Create a Mailbox Store

Step 1 Log on 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 click **Mailbox Stores**.

Step 3 On the Search Mailbox Store page, click **Add New**.

Step 4 On the New Mailbox Store page, enter settings as applicable.



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

Step 5 Click **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**.

Moving Mailboxes Between Mailbox Stores

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 log on to the server whose server status is primary to move mailboxes.
- Moving a mailbox fails if:
 - The administrator currently logged on 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 Log on 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 click **Mailbox Stores Membership**.
- Step 3** On the Search Mailbox Stores Membership page, in the Choose Membership Type list, click **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 click **Find**. The specified users appear in the table at the bottom of the page.
- Step 6** Choose 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** Click **Move Selected Mailboxes**.

Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged

Revised May 2009

To Change the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged

- Step 1** Log on 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 click **Mailbox Stores**.
- Step 3** On the Search Mailbox Store page, click 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** Click **Save**.

Deleting a Mailbox Store

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 Log on 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:

- In Cisco Unity Connection Administration, expand **Message Storage**, then click **Mailbox Stores Membership**.
- In the Choose Membership Type list, click **User Mailbox**.
- Under User Mailbox Search Results, specify the mailbox store from which you want to move mailboxes.
- Specify search criteria to further identify the users whose mailboxes you want to move, and click **Find**.

The specified users appear in the table at the bottom of the page.

- Choose the mailbox store to which you want to move mailboxes.
- Check the applicable check boxes to select the users whose mailboxes you want to move.
- Click **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:

- On the Search Mailbox Stores Membership page, in the Choose Membership Type list, click **User Template**.
- Under User Mailbox Search Results, choose the options to find the user templates that reference the mailbox store that you want to delete, and click **Find**.
- 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 click **Assign Selected Templates**.

Step 4 In Cisco Unity Connection Administration, expand **Message Storage**, then click **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 Click **Delete Selected**.

Step 7 Click **OK** to confirm.

Disabling and Re-Enabling a Mailbox Store

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.



CHAPTER 22

Controlling the Size of Mailboxes

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, page 22-1](#)
- [Changing the Message Aging Policy, page 22-2](#)

Specifying Mailbox Size Quotas

Revised May 2009

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, Connection is configured with the systemwide mailbox size quotas listed in [Table 22-1](#). To change systemwide quotas, do the “[To Change the Default Systemwide Quotas](#)” procedure on page 22-2.



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 System Settings > Advanced > Conversations 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](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Table 22-1 Mailbox-Size Quotas

Quota Level	Mailbox Size That Triggers Quota Action	Action When Quota Is Reached	Recording Time in Minutes Before Quota Is Reached				
			G.711 Mu-Law	G.711 A-Law	G.726 32 Kbps	PCM 8 kHz	G.729a
Warning	12 megabytes	The user is warned that the mailbox is reaching the maximum size allowed.	25	25	50	50	200
Send	13 megabytes	The user is prevented from sending any more voice messages.	27	27	54	54	217
Send/Receive	14 megabytes	The user is prevented from sending or receiving any more voice messages.	31	31	61	61	246

To Change the Default Systemwide Quotas

Step 1 In Cisco Unity Connection Administration, expand **Message Storage**, then click **Mailbox Quotas**.

Step 2 Set values for the following quotas, as applicable, by clicking **Custom** and then entering a value (in megabytes) in the adjacent field:

- Warning Quota
- Send Quota
- Send/Receive Quota

Note that 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 Click **Save**.

Changing the Message Aging Policy

Revised May 2009

To help ensure that the hard disk where voice messages are stored does not fill up, you can configure Cisco Unity Connection message aging rules to automatically:

- Move read messages to the Deleted Items folder after a specified number of days. This rule is disabled by default.
- Permanently delete messages in the Deleted Items folder after a specified number of days. This rule is enabled by default.
- 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). This rule is disabled by default.
- 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. This rule is disabled by default.

You can enable or disable these message aging rules, and you can specify a different number of days for each rule. You can also enable or disable the message aging policy; disabling the policy means that the rules are not enforced regardless of their settings.

If the message aging policy is enabled, and if one or more message aging rules are enabled, you can still disable message aging for individual users on the Voice Mailbox page. However, if the message aging policy is disabled, you cannot enable it for individual users.

Some of the message aging rules are based on when a message was last modified. To modify the status of a message, a user must do one of the following:

- In the Cisco Unity Inbox, mark the message as new, mark the message as deleted, or change the message subject, and click **Save**.
- From the phone interface, choose 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 status of the message.

To Change the Message Aging Policy

-
- Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then click **Message Aging Policy**.
- Step 2** Change settings as applicable. See Help for information on individual fields.
- Step 3** Click **Save**.
-

When the message aging policy is enabled for Connection, you can enable or disable the message aging policy for individual users and templates. (By default, user templates specify that message aging is enabled for users.)

For information on changing the message aging policy for individual users and for templates, see the “[Message Aging](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.



CHAPTER 23

Setting Up SMTP and SMS (SMPP) Message Notifications

Cisco Unity Connection can notify a user of new messages by calling a phone or pager. Additionally, you can set up Connection to send message and calendar event notifications in the form of text messages to text pagers and text-compatible cell phones by using SMTP. You can also set up 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 SMTP Message Notifications, page 23-1](#)
- [Setting Up SMS \(SMPP\) Message Notifications, page 23-2](#)

(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” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.)

Setting Up SMTP Message Notifications

Revised May 2009

By using SMTP, Cisco Unity Connection can send text notification to notify users that they have received a new message or calendar event. Text notifications can be sent to any device that supports SMTP, for example, email addresses, cell phones, and text pagers.

To enable Connection to send text notifications by using SMTP, your Connection server must be configured to relay messages through a smart host. If Connection is configured to deliver 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 Connection SMTP Server badmail folder.

When a Connection user receives a new message, Connection can send a text notification to an email address. (When you set up this type of notification, you can configure Connection to include a link to the Cisco PCA in the body of the email message. On the Edit Notification Device page for the user, check the Include a Link to Cisco PCA in Message Text check box.)

To enable SMTP notifications, do the following tasks:

1. Configure the SMTP smart host to accept messages from the Connection server. See the documentation for the SMTP server application that you are using.
2. Configure the Connection server. See the “[To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host](#)” procedure on page 23-2.

3. Configure Connection users or templates. See the “[SMTP-Compatible Notification Devices](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Alternatively, users can set up their own SMTP-compatible devices by using the Cisco Unity Assistant.

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 click **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. (Enter the fully qualified domain name of the server only if DNS is configured.)
 - Step 3** Click **Save**.
-

Setting Up SMS (SMPP) Message Notifications

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 cell 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 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 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 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 cell 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 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 Cisco Unity Assistant that Connection sends message notifications only when new urgent voice messages arrive.

Task List for Setting Up SMS (SMPP) Message Notifications

Revised May 2009

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. 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 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 23-4](#).
3. When the Connection server is set up behind a firewall, configure the TCP port that is used by the SMPP server when connecting to Connection to allow incoming and outgoing communication between Connection and the SMPP server.
4. Enable SMS (SMPP) message notification and set up an SMS-compatible device to receive them 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”](#) chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

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 click **SMPP Providers**.
- Step 2** On the Search SMPP Providers page, click **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. Click **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** Click **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.
- 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** Click **Save**.
-



CHAPTER 24

Securing User Messages: Controlling Access and Distribution

By setting message sensitivity, users can control who can access a voice message and whether it can be redistributed to others. Cisco Unity Connection also offers ways for you to prevent users from saving voice messages as WAV files to their hard drives or other locations outside the Connection server, enabling you to maintain control of how long messages are retained before they are archived or purged.

See the following sections:

- [How Cisco Unity Connection Handles Messages That Are Marked Private or Secure, page 24-1](#)
- [Disabling the “Save Recording As” Option in the Media Master for All Voice Messages, page 24-3](#)
- [Message Security Options for IMAP Client Access, page 24-3](#)

How Cisco Unity Connection Handles Messages That Are Marked Private or Secure

Revised May 2009

When users send messages by phone in Cisco Unity Connection, the messages can be marked private, secure, or both private and secure. You can also specify whether Connection marks messages that are left by outside callers as secure.

Private Messages

- Any recipient can receive a private message—including non-Connection users. Recipients can use the phone, the Cisco Unity Inbox, Cisco Unified Personal Communicator, Cisco Unified Messaging with IBM Lotus Sametime, or an IMAP client to listen to private messages.
- Private messages cannot be forwarded by phone or from the Cisco Unity Inbox.
- A private message can be forwarded and can be saved locally as a WAV file when accessed from an IMAP client unless you specify otherwise. (See the [“Message Security Options for IMAP Client Access” section on page 24-3](#) to learn how to prohibit users from playing and forwarding private messages and from saving private messages as WAV files.)
- When users reply to a private message, the reply is marked normal.
- When users send a message, they can choose to mark it private.
- When outside callers leave messages for users, they cannot mark them private.

- When users do not explicitly log on to their mailboxes before leaving messages for other users, they cannot mark the messages private.

Secure Messages

- Secure messages are stored only on the Connection server, allowing you to control how long messages are retained before they are archived or purged. For secure messages, the Save Recording As option is automatically disabled on the Options menu on the Media Master in the Cisco Unity Inbox, Cisco Unity Connection ViewMail for Microsoft Outlook, and Cisco Unity Connection ViewMail for IBM Lotus Notes.
- Secure messages can be useful for enforcing your message retention policy. You can configure Connection to automatically delete secure messages that are older than a specified number of days, regardless of whether users have listened to or touched the messages in any way. For more information, see the “[Changing the Message Aging Policy](#)” section on page 22-2.
- Secure messages can be played by using the following interfaces:
 - Connection phone interface
 - Cisco Unity Inbox
 - Cisco Unity Connection ViewMail for Microsoft Outlook
 - Cisco Unity Connection ViewMail for IBM Lotus Notes
 - Cisco Unified Personal Communicator version 7.0 and later
 - Cisco Unified Messaging with IBM Lotus Sametime version 7.1.1 and later. (For requirements for playing secure messages using Cisco Unified Messaging with Lotus Sametime, see the applicable *Release Notes for Cisco Unified Messaging with IBM Lotus Sametime* at http://www.cisco.com/en/US/products/ps9830/prod_release_notes_list.html.)
- Secure messages cannot be accessed by using the following interfaces:
 - IMAP clients (unless Cisco Unity Connection ViewMail for Microsoft Outlook or Cisco Unity Connection ViewMail for IBM Lotus Notes is installed)
 - RSS readers
- Only Connection users can receive a secure message. (VPIM contacts may also be able to receive the message, but only when the VPIM location is configured to change the message sensitivity to normal before delivering it.)
- Replies to secure messages are also marked secure.
- A secure message can be forwarded to other Connection users and to the Connection users in a distribution list. The forwarded message is also marked secure. Users cannot change the sensitivity of forwarded messages and replies.
- When users log on to Connection and send a message, class of service settings determine whether the message is marked secure. By default, Connection automatically marks a message secure when the user marks it private.
- When callers are routed to a user or call handler greeting and then leave a message, the Mark Messages Secure check box on the Edit > Message Settings page for a user or call handler account determines whether Connection marks the message secure.

Disabling the “Save Recording As” Option in the Media Master for All Voice Messages

By default, except for messages that are marked private, secure, or private and secure, users can save their messages as WAV files to their hard disks by using the Save Recording As option, available on the Media Master Options menu in the Cisco Unity Inbox. You can prevent users from saving any voice message—regardless of its sensitivity—by disabling the Save Recording As option on the Options menu of the Media Master in the Cisco Unity Inbox.

Note the following as you consider this security option:

- When you prevent users from by saving messages to their hard disks, they may choose to retain them in their Inboxes and Deleted Items folders longer as a way of archiving them.
- Disabling the Save Recording As option affects all users who are associated with the Connection server; you cannot disable it only for individual users.
- Users can continue to use the Media Master to save greetings or recorded names as WAV files.

To Disable the Save Recording As Option in the Media Master in the Cisco Unity Inbox

-
- | | |
|---------------|--|
| Step 1 | In Cisco Unity Connection Administration, expand System Settings > Advanced , then click PCA . |
| Step 2 | On the PCA Configuration page, check the Unity Inbox: Disable Save Recording As Option in Media Master check box. |
| Step 3 | Click Save . |
-

Message Security Options for IMAP Client Access

When users access voice messages that are marked with normal or private sensitivity from an IMAP client, the IMAP client may allow users to save messages as WAV files to their hard disks, and may allow users to forward the messages. To prevent users from saving and/or forwarding voice messages from their IMAP client, consider specifying one of the following class of service options:

- Users can only access message headers in an IMAP client—regardless of message sensitivity.
- Users can access message bodies for all messages except those that are marked private. (Secure messages cannot be accessed in an IMAP client, unless the client is Microsoft Outlook and ViewMail for Outlook is installed or the client is Lotus Notes and ViewMail for Notes is installed.)



CHAPTER 25

Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection

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 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 Connection. Note that IMAP client access to Connection voice messages is a licensed feature.

See the following sections:

- [Deciding Whether to Create and Install an SSL Certificate, page 25-1](#)
- [Creating and Installing an SSL Server Certificate, page 25-2](#)

Deciding Whether to Create and Install an SSL Certificate

When you install Cisco Unity Connection, a local certificate is automatically created and installed to secure communication between the Cisco PCA and Connection, and between IMAP email clients and Connection. This means that all network traffic (including user names, passwords, other text data, and voice messages) between the Cisco PCA and Connection is automatically encrypted, and network traffic between IMAP email clients and 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 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](#)” section in the “Setting Up Access to the Cisco Personal Communications Assistant” chapter of the *User Workstation Setup Guide for Cisco Unity Connection*. For information on configuring supported IMAP email clients, see the “[Configuring an Email Account to Access Cisco Unity Connection Voice Messages](#)” chapter of the same guide.)

Creating and Installing an SSL Server Certificate

Revised May 2009

Do the following tasks to create and install an SSL server certificate to secure 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. Do the [“To Install the Microsoft Certificate Services Component” procedure on page 25-3](#).
If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Step 2.
If you are using an external certification authority to issue certificates, skip to Step 2.



Note

If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Step 2.

2. If a Connection cluster is configured, run the `set web-security` CLI command on both 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 Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Step 2. List the publisher server first. This allows all IMAP email applications and the Cisco Personal Communications Assistant to access Connection voice messages by using the same 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 25-3](#).
If a Connection cluster is configured, do this step for both servers in the Connection cluster.
5. If you are using Microsoft Certificate Services to export the issuer certificate and to issue the server certificate, do the [“To Export the Issuer Certificate and to Issue the Server Certificate \(Only When You Are Using Microsoft Certificate Services to Issue the Certificate\)” procedure on page 25-4](#).
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 Step 6.
If a Connection cluster is configured, do this step for both servers in the Connection cluster.
6. Upload the issuer certificate and the server certificate to the Connection server. Do the [“To Upload the Issuer and Server Certificates to the Cisco Unity Connection Server” procedure on page 25-5](#).
If a Connection cluster is configured, do this step for both servers in the Connection cluster.
7. Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the [“To Restart the Connection IMAP Server Service” procedure on page 25-6](#).
If a Connection cluster is configured, do this step for both servers in the Connection cluster.

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, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.
- Step 3** In the left pane of the Add or Remove Programs control panel, click **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, click **Yes**.
- Step 6** Click **Next**.
- Step 7** On the CA Type page, click **Stand-alone Root CA**, and click **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** Click **Next**.
- Step 12** On the Certificate Database Settings page, click **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, click **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, click **Finish**.
- Step 15** Close the Add or Remove Programs dialog box.
-

To Create and Download a Certificate Signing Request

- Step 1** On the Cisco Unity Connection server, log on to Cisco Unified Operating System Administration.
- Step 2** On the Security menu, click **Certificate Management**.
- Step 3** On the Certificate List page, click **Generate CSR**.
- Step 4** On the Generate Certificate Signing Request page, in the **Certificate Name** list, click **tomcat**.
- Step 5** Click **Generate CSR**.
- Step 6** When the Status area displays a message that the CSR was successfully generated, click **Close**.
- Step 7** On the Certificate List page, click **Download CSR**.
- Step 8** On the Download Certificate Signing Request page, in the **Certificate Name** list, click **tomcat**.
- Step 9** Click **Download CSR**.
- Step 10** In the File Download dialog box, click **Save**.
- Step 11** In the Save As dialog box, in the **Save As Type** list, click **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, click **Close**.

To Export the Issuer Certificate and to Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

- Step 1** On the server on which you installed Microsoft Certificate Services, log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **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 25-3](#).
- Step 4** Export the issuer certificate:
- Right-click the name of the certification authority, and click **Properties**.
 - On the General tab, click **View Certificate**.
 - Click the **Details** tab.
 - Click **Copy to File**.
 - On the Welcome to the Certificate Export Wizard page, click **Next**.
 - On the Export File Format page, click **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.
 - On the File to Export page, enter a path and file name for the .cer file. Choose a network location that you can access from the Connection server.
Write down the path and file name. You will need it in a later procedure.
 - Follow the onscreen prompts until the wizard has finished the export.
 - Click **OK** to close the Certificate dialog box, and click **OK** again to close the Properties dialog box.
- Step 5** Issue the server certificate:
- Right-click the name of the certification authority, and click **All Tasks > Submit New Request**.
 - 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 25-3](#), and double-click the file.
 - In the left pane of Certification Authority, click **Pending Requests**.
 - Right-click the pending request that you submitted in [b.](#), and click **All Tasks > Issue**.
 - In the left pane of Certification Authority, click **Issued Certificates**.
 - Right-click the new certificate, and click **All Tasks > Export Binary Data**.
 - In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, click **Binary Certificate**.
 - Click **Save Binary Data to a File**.
 - Click **OK**.

- j. In the Save Binary Data dialog box, enter a path and file name. Choose a network location that you can access from the Cisco Unity Connection server.

Write down the path and file name. You will need it in a later procedure.

- k. Click **OK**.

Step 6 Close Certification Authority.

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, log on to Cisco Unified Operating System Administration.

Step 2 On the Security menu, click **Certificate Management**.



Note If you click **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, click **Upload Certificate**.
- b. On the Upload Certificate page, in the Certificate Name list, click **tomcat-trust**.
- c. Leave the Root Certificate field blank.
- d. Click **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 \(Only When You Are Using Microsoft Certificate Services to Issue the Certificate\)” procedure on page 25-4](#).

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. Click the name of the file.
- f. Click **Open**.
- g. On the Upload Certificate page, click **Upload File**.
- h. When the Status area reports that the upload succeeded, click **Close**.

Step 4 Upload the server certificate:

- a. On the Certificate List page, click **Upload Certificate**.
- b. On the Upload Certificate page, in the Certificate Name list, click **tomcat**.
- c. In the Root Certificate field, enter the filename of the issuer certificate that you uploaded in [Step 3](#).
- d. Click **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 \(Only When You Are Using Microsoft Certificate Services to Issue the Certificate\)” procedure on page 25-4](#).

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. Click the name of the file.
- f. Click **Open**.
- g. On the Upload Certificate page, click **Upload File**.
- h. When the Status area reports that the upload succeeded, click **Close**.

Step 5 Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

- a. Log on to the 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 Connection IMAP Server Service

Step 1 Log on to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, click **Service Management**.

Step 3 In the Optional Services section, for the Connection IMAP Server service, click **Stop**.

Step 4 When the Status area displays a message that the Connection IMAP Server service was successfully stopped, click **Start** for the service.



CHAPTER 26

Setting Up Broadcast Messaging

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, page 26-1](#)
- [Task List for Offering Broadcast Messaging to Users, page 26-2](#)
- [Enabling Phone Access to the Broadcast Message Administrator, page 26-2](#)
- [Using the Broadcast Message Administrator, page 26-5](#)
- [Changing Broadcast Message Administrator Defaults, page 26-6](#)

How System Broadcast Messages Work

Revised May 2009

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 log on to Cisco Unity Connection by phone—even before they hear message counts for new and saved messages. After logging on, users hear how many system broadcast messages they have and Connection begins playing them.
- For each system broadcast message, the sender specifies how long 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 logs on to Connection during the period that the message is active.
- Users must listen to a system broadcast message in its entirety before 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 logs on to 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 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 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 Inbox, an RSS reader, IMAP clients, Cisco Unified Personal Communicator, or Cisco Unified Messaging with IBM Lotus Sametime.
- 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

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”](#) section on page 26-2.
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”](#) chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Enabling Phone Access to the Broadcast Message Administrator

Revised May 2009

To send a system broadcast message, Cisco Unity Connection users log on 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”](#) chapter for details.
- Create a call handler—See the [“Creating a Call Handler to Send Users to the Broadcast Message Administrator”](#) section on page 26-3.
- 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 26-3.
- 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 26-5.

Creating a Call Handler to Send Users to the Broadcast Message Administrator

Revised May 2009

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 click System Call Handlers . |
| Step 2 | On the Search Call Handlers page, click 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 | Click Save . |
| Step 6 | On the Edit Call Handler Basics page, on the Edit menu, click Greetings . |
| Step 7 | On the Greetings page, click the Standard greeting. |
| Step 8 | On the Edit Greeting page, in the Callers Hear section, click Nothing . (Alternatively, you can click My Personal Recording and record a greeting that introduces the caller to the Broadcast Message Administrator conversation.) |
| Step 9 | In the After Greeting section, click Conversation and then click Broadcast Message Administrator . |
| Step 10 | Click 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 26-4 . |
-

Setting Up a One-Key Dialing Option to Send Users to the Broadcast Message Administrator



Revised May 2009

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 26-4](#)
- [To Set Up a One-Key Dialing Option from a User Greeting for Accessing the Broadcast Message Administrator, page 26-4](#)

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 click **System Call Handlers**.
- Step 2** On the Search Call Handlers page, in the Search Results table, click the display name of the applicable call handler.
- If you want to set up access to the Broadcast Message Administrator from the opening greeting, click the **Opening Greeting** call handler. Or click 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 click **Find**.
- Step 3** On the Edit Call Handler Basics page, on the Edit menu, click **Caller Input**.
- Step 4** On the Caller Input page, in the Caller Input Keys table, click 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** Click **Conversation**, and then click **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** Click **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, click **Users**.
- Step 2** On the Search Users page, in the Search Results table, click 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 click **Search**.
- Step 3** On the Edit User Basics page, on the Edit menu, click **Caller Input**.
- Step 4** On the Caller Input page, in the Caller Input Keys table, click 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** Click **Conversation**, and then click **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** Click **Save**.
-

Setting Up a Special Phone Number and Routing Rule to Send Users to the Broadcast Message Administrator

Revised May 2009

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 click **Direct Routing Rules**.
- Step 2** On the Direct Routing Rules page, click **Add New**.
- Step 3** On the New Direct Routing Rule page, enter a display name for the new routing rule, and click **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, click **Conversation**, and then click **Broadcast Message Administrator**.
- Step 6** Click **Save**.
- Step 7** In the Routing Rule Conditions table, click **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** Click **Save**.
- Step 10** On the Direct Routing Rule menu, click **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** Click **Change Order**.
- Step 13** On the Edit Direct Routing Rule Order page, click the name of the rule you want to reorder, and click the Up or Down arrow until the rules appear in the correct order. Click **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

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” section on page 26-6](#).

Note that 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 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 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 Connection does not report which users have already played an active message.)

Changing Broadcast Message Administrator Defaults

Revised May 2009

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 Connection retains expired system broadcast messages on the server. By default, 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 Connection presents system broadcast messages to users. By default, the check box is checked, which sets Connection to play the oldest message first. To have the newest message played first, uncheck the check box.



CHAPTER 27

Managing System Distribution Lists

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, page 27-1](#)
- [Creating System Distribution Lists, page 27-2](#)
- [Modifying System Distribution Lists, page 27-3](#)
- [Managing System Distribution List Members, page 27-3](#)
- [Adding Alternate Names for a System Distribution List, page 27-4](#)

Predefined System Distribution Lists

Revised May 2009

Cisco Unity Connection includes the following predefined system distribution lists, which you can modify but not delete:

All Voice Mail Users	<p>When users with mailboxes are created, they are automatically added to the All Voice Mail Users list.</p> <p>When user accounts are deleted, they are automatically removed from this distribution list.</p> <div>Note Default user accounts are not members of this list.</div>
-----------------------------	---

Undeliverable Messages	<p>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.</p> <p>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.</p>
All Voicemail-Enabled Contacts	<p>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.</p>

Creating System Distribution Lists

Revised May 2009

To Create a System Distribution List

- Step 1** In Cisco Unity Connection Administration, expand **Distribution Lists**, then click **System Distribution Lists**.
- Step 2** On the Search Distribution Lists page, click **Add New**.
- Step 3** On the New Distribution List page, enter an alias and display name for the list.
- Step 4** Click **Save**.
- Step 5** On the Edit Distribution List Basics page, use the Media Master to record a voice 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** Click **Save**.
- Step 8** On the Edit Menu, click **Distribution List Members**.
- Step 9** On the Distribution List Members page, click **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 click **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 click **Find** to display additional names in the table.

- Step 11** When you have added all members to the list, click **Close**.

**Note**

You may need to click **Refresh** on the menu bar to see an updated list of distribution list members in the table.

Modifying System Distribution Lists

To Modify a System Distribution List

Step 1 In Cisco Unity Connection Administration, expand **Distribution Lists**, then click **System Distribution Lists**.

Step 2 On the Search Distribution Lists page, click 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 click **Find**.

Step 3 On the Edit Distribution List Basics page, change settings as applicable.

Step 4 Click **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.

Managing System Distribution List Members

You can add individual users directly to system distribution lists. When you delete a user account, Connection automatically removes the user from any system distribution list of which the user is a member.

To Add or Remove Users from a System Distribution List

Step 1 In Cisco Unity Connection Administration, expand **Distribution Lists**, then click **System Distribution Lists**.

Step 2 On the Search Distribution Lists page, click 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 click **Find**.

Step 3 On the Edit Distribution List Basics page, on the Edit menu, click **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, click **Add User**.



Note You can also add other distribution lists as members of a distribution list. To add a distribution list, click **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 click **Add Selected**.
- Step 7** Click **Close**.
- Step 8** To see the updated list of members, on the menu bar, click **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 click **Remove Selected**.

Adding Alternate Names for a System Distribution List

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 click **System Distribution Lists**.
- Step 2** On the Search Distribution Lists page, click 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 click **Find**.

- Step 3** On the Edit Distribution List Basics page, on the Edit menu, click **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 click **Add New**. When you have finished adding new alternate names, click **Save**.
 - To modify an existing alternate name, in the Edit Alternate Names table, change the display name, then click **Save**.
 - To delete an alternate name, check the check box next to the name, click **Delete Selected**, then click **OK** to verify that you want to delete the name.



CHAPTER 28

Managing Partitions and Search Spaces

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: Partitions, page 28-1](#)
- [Overview: Search Spaces, page 28-2](#)
- [Default Partition and Search Space, page 28-2](#)
- [Search Space Examples, page 28-3](#)
- [How Search Spaces Work in Cisco Unity Connection, page 28-5](#)
- [Managing Partitions, page 28-8](#)
- [Managing Search Spaces, page 28-9](#)
- [Changing the System Default Partition and Search Space, page 28-11](#)
- [Finding Objects that Belong to a Partition or Search Space, page 28-11](#)

Overview: Partitions

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 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. System 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.

Overview: Search Spaces

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 system 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 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, 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

When you install or upgrade to Cisco Unity Connection release 7.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, 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”](#) section on page 28-11.)

Search Space Examples

See the following sections:

- [Single Site Automated Attendant Search Space Example, page 28-3](#)
- [Multiple Site Search Space Example, page 28-4](#)

Single Site Automated Attendant Search Space Example

Revised May 2009

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 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 Connection are configured to use the Employees-SS as their search space.

In this example, when users call and log on to Connection, they can address messages or place calls to any other user at the company. However, when outside callers call Connection and reach the automated attendant, they can only reach 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, 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 log in to Connection and attempt to reach extension 411, 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

Revised May 2009

CompanyB has three digitally networked Cisco Unity Connection locations serving three sites: Headquarters, Regional-East, and Regional-West.

The configuration is as follows:

- 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. (In Connection 7.0, the Dial ID field was named DTMF Access ID.)
- 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, Connection users can address other 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, Connection returns Chris Brown as the match. If Alex addresses a message by spelling SMITHR on the phone keypad (764847), Connection returns both Pat Smith and Robin Smith, because both names match the 764847 spelling. If Alex addresses a message by saying “Robin Smith,” 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 log on to Connection. (For information about setting up cross-server logon and transfers, see the [“Using Digital Networking”](#) chapter.)

How Search Spaces Work in Cisco Unity Connection

See the following sections for details on the interactions between search spaces and various Connection concepts:

- [Search Spaces and Users, page 28-5](#)
- [Search Spaces and Call Routing Rules, page 28-6](#)
- [Search Spaces and System Distribution Lists, page 28-6](#)
- [Search Spaces and System Call Handlers, page 28-7](#)
- [Search Spaces and Directory Handlers, page 28-7](#)
- [Search Spaces and Interview Handlers, page 28-7](#)
- [Search Spaces and Digital Networking, page 28-7](#)
- [Search Spaces and VPIM Locations, page 28-8](#)
- [Search Spaces and System Contacts, page 28-8](#)

Search Spaces and Users

When a user has logged on 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. Connection applies the search scope of the user whether the user is interacting with 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, 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 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 Connection or was forwarded from an extension. When 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:

- 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 Connection finds when searching the partitions in the order that they appear in the search space.
- Users who call to log on to Connection do not have their search scope set to the search space defined for their user profile until they have successfully completed the logon process.

If users are segmented into different partitions, and extensions overlap between partitions, you must consider how Connection recognizes users by extension when they call 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 Connection from extension 3001, 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, system 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 Digital Networking

Revised May 2010

When you network a Cisco Unity Connection server with other Connection locations, the partitions and search spaces that are configured on the server replicate to all other Connection locations on the network.

If you plan to use digital networking to connect multiple Connection servers, it is important to note that when you initially set up digital networking 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 Connection server to the search space that local users are using.

Search Spaces and VPIM Locations

Revised May 2009

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. (In Connection 7.0, the Dial ID field was named DTMF Access ID.)

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 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 Connection user.

Each VPIM location also has a search scope. When Connection receives a message from a sender at a VPIM location, 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 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 System Contacts

Each system 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

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 click **Partitions**.
 - Step 2** On the Search Partitions page, click **Add New**.
 - Step 3** On the New Partition page, enter a name for the partition.

Step 4 Click **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 click **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 click **Partitions**.

Step 2 On the Search Partitions page, click 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 click **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, click **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 find and move all users in a partition to another partition, see the [“Finding Users Based on Partition or Search Space in the Cisco Unity Connection Bulk Edit Utility”](#) section on page 28-12.)

To Delete a Partition

Step 1 In Cisco Unity Connection Administration, expand **Dial Plan**, then click **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 click **Find**.

Step 3 Click **Delete Selected**, and click **OK** to confirm the deletion.

Managing Search Spaces

Revised May 2009

To Create a Search Space

- Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then click **Search Spaces**.
 - Step 2** On the Search Search Spaces page, click **Add New**.
 - Step 3** On the New Search Space page, enter a name for the search space.
 - Step 4** Click **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, click the name of the partition in the Unassigned Partitions list, then click the Up arrow above the list.
 - Step 7** To change the order of partitions in the Assigned Partitions list, click the name of the partition to move, then click the Up or Down arrow to the right of the list.
 - Step 8** When you are done modifying the partition membership, click **Save**.
-

To Modify a Search Space

- Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then click **Search Spaces**.
 - Step 2** On the Search Search Spaces page, click 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, click the name of the partition in the Unassigned Partitions list, then click the Up arrow above the list.
 - Step 5** To change the order of partitions in the Assigned Partitions list, click the name of the partition to move, then click 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, click **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 click **Search Spaces**.
- Step 2** On the Search 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 click **Find**.

- Step 3** Click **Delete Selected**, and click **OK** to confirm the deletion.
-

Changing the System Default Partition and Search Space

Revised May 2009

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 that 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 click General Configuration . |
| Step 2 | On the Edit General Configuration page, in the Default Partition field, click the name of the new default partition. |
| Step 3 | In the Default Search Scope field, click the name of the new default search space. |
| Step 4 | Click Save . |
-

Finding Objects that Belong to a Partition or Search Space

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 28-11](#)
- [Finding Users Based on Partition in Cisco Unity Connection Serviceability, page 28-12](#)
- [Finding Users Based on Partition or Search Space in the Cisco Unity Connection Bulk Edit Utility, page 28-12](#)

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, click Partition . |
| Step 3 | In the Where Name Is list, click the name of the partition in which to find objects. |

**Note**

When searching for users, you can also choose 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 choose 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. Click **Find**.

Finding Users Based on Partition in Cisco Unity Connection Serviceability

Revised May 2009

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 7.x*, at

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/serv_administration/guide/7xcucservagx.html.

Finding Users Based on Partition or Search Space in the Cisco Unity Connection Bulk Edit Utility

The Cisco Unity Connection Bulk Edit utility allows you to select user accounts based on partition membership or search scope.

You can use the Bulk Edit utility to move users between partitions or change the search scope of multiple users at one time.

To Find Users Based on Partition or Search Space in the Cisco Unity Connection Bulk Edit Utility

- Step 1** In Cisco Unity Connection Administration, expand **Tools**, then click **Bulk Edit Utility**.
- Step 2** Click **Users with Voice Mail**.
- Step 3** To locate users in a particular partition, in the Select Users list, click **Users in This Partition**, then click the name of the partition and click **Find**.
- Or, to locate users with a particular search scope, in the Select Users list, click **Users With Search Scope**, then click the name of the search space and click **Find**.



CHAPTER 29

Managing the Phone System Integrations

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, page 29-1](#)
- [Managing Port Groups, page 29-7](#)
- [Managing Ports, page 29-17](#)
- [Managing Phone System Trunks, page 29-20](#)
- [Security \(Cisco Unified Communications Manager Integrations Only\), page 29-22](#)

Managing Phone Systems

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 29-2](#)
- [Deleting a Phone System Integration, page 29-2](#)
- [Changing Phone System Settings, page 29-3](#)
- [Listing the Users Who Are Associated with the Phone System, page 29-3](#)
- [Disabling the Use of the Same Port for Turning On and Off an MWI, page 29-3](#)
- [Synchronizing MWIs for the Phone System, page 29-4](#)
- [Configuring Phone View Settings \(Cisco Unified Communications Manager Integrations Only\), page 29-4](#)
- [Changing Call Loop Detection Settings, page 29-4](#)
- [Managing AXL Servers, page 29-5](#)

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 click **Phone System**.
 - Step 2** On the Search Phone Systems page, under Phone System Search Results, click **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 click **Save**.
 - Step 4** On the Phone System Basics page, enter the applicable settings and click **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 29-3](#).

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 click **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** Click **Delete Selected**.

- Step 4** When prompted to confirm that you want to delete the phone systems, click **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 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 click **Phone System**.
- Step 2** On the Search Phone Systems page, click 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 click **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 click **Phone System**.
- Step 2** On the Search Phone Systems page, click the display name of the phone system.
- Step 3** On the Phone System Basics page, on the Edit menu, click **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 click **Phone System**.
- Step 2** On the Search Phone Systems page, click 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 click **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 click **Save**.
 - Step 5** Click **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 click **Phone System**.
 - Step 2** On the Search Phone Systems page, click the display name of the phone system.
 - Step 3** On the Phone System Basics page, click **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”](#) chapter.

To Configure Phone View Settings (Cisco Unified Communications Manager Integrations Only)

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
 - Step 2** On the Search Phone Systems page, click the display name of the phone system.
 - Step 3** On the Phone System Basics page, under Phone View Settings, enter the applicable settings and click **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 Connection. When call loop detection is enabled, 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 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 Connection forwards.

To Change Call Loop Detection Settings

-
- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 2** On the Search Phone Systems page, click 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 click **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 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 Connection cluster is configured, you must be logged on to the publisher server of the Connection cluster to import Cisco Unified CM user data.

See the following procedures:

- [To Add AXL Servers, page 29-5](#)
- [To Delete an AXL Server, page 29-7](#)
- [To Change AXL Server Settings, page 29-7](#)

To Add AXL Servers

-
- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 2** On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.
- Step 3** On the Phone System Basics page, on the Edit menu, click **Cisco Unified Communications Manager AXL Servers**.
- Step 4** On the Edit AXL Servers page, under AXL Servers, click **Add New**.
- Step 5** Enter the following settings for the AXL server and click **Save**.

Table 29-1 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 Connection connects to. This setting must match the port that the AXL server uses. For Cisco Unified Communications Manager version 4.1(x), the port number is typically 443. 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 click **Save**.

Table 29-2 Settings for the AXL Server Settings

Field	Setting
User Name	Enter the user name that Connection uses to log on to the AXL server. Note This user must match the user name of a Cisco Unified CM application user who is assigned to the “Standard AXL API Access” role.
Password	Enter the password for the user that Connection uses to log on to the AXL server. Note This password must match the password of the Cisco Unified CM application user entered in the User Name field.
Cisco Unified Communications Manager Version	Select the Cisco Unified CM version in the list: <ul style="list-style-type: none"> Pre 5.0 (Non-SSL) Pre 5.0 (SSL) 5.0 or Greater (SSL) <p>If you select the Pre 5.0 (Non-SSL) version, the AXL port must be a non-SSL port (typically port 80).</p> <p>If you select the Pre 5.0 (SSL) version, the AXL port must be an SSL-enabled port (typically port 443 with Pre 5.0 versions).</p> <p>If you select the 5.0 or Greater (SSL) version, the AXL port must be an SSL-enabled port (typically port 8443).</p>

**Caution**

After the changes to this page are saved, you can click **Test** (next to the AXL server port number) to verify the connection to the AXL server. If the AXL port that you enter and the Cisco Unified CM Version setting conflict concerning whether SSL is used, the results of the test require more than 10 minutes to appear.

Step 8 To add a corresponding application server to Cisco Unified CM, log on 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, click **Find** to display all application servers.
- Step 11** In the Name column, click 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 click the **Down** arrow to move it to the Selected Application User field.
- Step 13** Click **Save**.
-

To Delete an AXL Server

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 2** On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.
- Step 3** On the Phone System Basics page, on the Edit menu, click **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** Click **Delete Selected**.
- Step 6** When prompted to confirm that you want to delete the AXL server, click **OK**.
-

To Change AXL Server Settings

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 2** On the Search Phone Systems page, click the display name of the Cisco Unified CM phone system.
- Step 3** On the Phone System Basics page, on the Edit menu, click **Cisco Unified Communications Manager AXL Servers**.
- Step 4** On the Edit AXL Servers page, change the applicable settings and click **Save**.
-

Managing Port Groups

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.

Connection port groups provide flexibility for integration configuration settings that apply to different sets of port.

See the following sections:

- [Adding a Port Group, page 29-8](#)
- [Deleting a Port Group, page 29-9](#)
- [Changing Port Group Settings, page 29-9](#)
- [Changing the Audio Format That Cisco Unity Connection Uses for Calls, page 29-9](#)
- [Changing MWI Settings, page 29-10](#)
- [Adding Secondary Cisco Unified Communications Manager Servers, page 29-10](#)
- [Deleting Cisco Unified Communications Manager Servers, page 29-11](#)
- [Changing Cisco Unified Communications Manager Server Settings, page 29-11](#)
- [Adding a TFTP Server, page 29-12](#)
- [Deleting a TFTP Server, page 29-12](#)
- [Changing TFTP Server Settings, page 29-13](#)
- [Adding a SIP Server, page 29-13](#)
- [Deleting a SIP Server, page 29-14](#)
- [Changing SIP Server Settings, page 29-14](#)
- [Managing PIMG/TIMG Units, page 29-15](#)
- [Changing Session Initiation Protocol \(SIP\) Settings, page 29-16](#)
- [Changing Port Group Advanced Settings, page 29-16](#)
- [Changing Automatic Gain Control \(AGC\) Settings, page 29-17](#)

Adding a Port Group

You can add multiple port groups, each with its own integration configuration settings and its own voice messaging ports.

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.

To Add a Port Group

-
- | | |
|---------------|---|
| Step 1 | In Cisco Unity Connection Administration, expand Telephony Integrations , then click Port Group . |
| Step 2 | On the Search Port Groups page, under Port Group Search Results, click Add New . |
| Step 3 | On the New Port Group page, enter the applicable settings and click 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 click 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 | Click Delete Selected . |
| Step 4 | When prompted to confirm that you want to delete the port group, click 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 click Port Group . |
| Step 2 | On the Search Port Groups page, click 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 click 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:

- 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 Connection server and on the phone system.
 - To preserve the audio quality of calls.
- When 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 click Port Group . |
|---------------|---|

- Step 2** On the Search Port Groups page, click 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, click **Codec Advertising**.
- Step 4** On the Edit Codec Advertising page, click 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, 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** Click **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, click the applicable packet setting for each codec and click **Save**.
- Step 7** Click **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 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 click **Port Group**.
- Step 2** On the Search Port Groups page, click 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 click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **Servers**.
 - Step 4** On the Edit Servers page, under Cisco Unified Communications Manager Servers, click **Add**.
 - Step 5** Enter the settings for the secondary Cisco Unified CM server and click **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 click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **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** Click **Delete Selected**.
 - Step 6** When prompted to confirm that you want to delete the Cisco Unified CM servers, click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **Servers**.
 - Step 4** On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and click **Save**.
-

**Note**

You can click **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 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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **Servers**.
 - Step 4** On the Edit Servers page, under TFTP Servers, click **Add**.
 - Step 5** Enter the settings for the TFTP server and click **Save**.
 - Step 6** Repeat [Step 4](#) and [Step 5](#) for all remaining TFTP servers that you want to add.
-

**Note**

You can click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **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** Click **Delete Selected**.
 - Step 6** When prompted to confirm that you want to delete the TFTP server, click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **Servers**.
 - Step 4** On the Edit Servers page, under TFTP Servers, change the applicable settings and click **Save**.
-

**Note**

You can click **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 click **Port Group**.

- Step 2** On the Search Port Groups page, click 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, click **Servers**.
- Step 4** On the Edit Servers page, under SIP Servers, click **Add**.
- Step 5** Enter the settings for the SIP server and click **Save**.
- Step 6** Repeat [Step 4](#) and [Step 5](#) for all remaining SIP servers that you want to add.
-

**Note**

You can click **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 click **Port Group**.
- Step 2** On the Search Port Groups page, click 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, click **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** Click **Delete Selected**.
- Step 6** When prompted to confirm that you want to delete the SIP server, click **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 click **Port Group**.

- Step 2** On the Search Port Groups page, click 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, click **Servers**.
- Step 4** On the Edit Servers page, under SIP Servers, change the applicable settings and click **Save**.

**Note**

You can click **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 29-15](#)
- [To Delete PIMG/TIMG Units, page 29-15](#)
- [To Change PIMG/TIMG Settings, page 29-16](#)

To Add PIMG/TIMG Units

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.
- Step 2** On the Search Port Groups page, under Port Group Search Results, click **Add New**.
- Step 3** On the New Port Group page, in the Phone System field, click the phone system for which you want to add a PIMG/TIMG unit.
- Step 4** Enter the applicable settings and click **Save**.

To Delete PIMG/TIMG Units

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **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** Click **Delete Selected**.

To Change PIMG/TIMG Settings

-
- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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 click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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 click **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 click **Port Group**.
 - Step 2** On the Search Port Groups page, click 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, click **Advanced Settings**.
 - Step 4** On the Edit Advanced Settings page, under Port Group Advanced Settings, change the applicable settings and click **Save**.
-

Changing Automatic Gain Control (AGC) Settings

The automatic gain control (AGC) settings control the automatic value adjustments for recording messages. We recommend that AGC settings be left at their default values.

To Change AGC Settings

-
- | | |
|---------------|---|
| Step 1 | In Cisco Unity Connection Administration, expand Telephony Integrations , then click Port Group . |
| Step 2 | On the Search Port Groups page, click 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, click Advanced Settings . |
| Step 4 | On the Edit Advanced Settings page, under Automatic Gain Control (AGC) Settings, change the applicable settings and click Save . |
-

Managing Ports

The voice messaging ports let Cisco Unity Connection receive calls (for example, to record a message) and let 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 Connection license files.

See the following sections:

- [Adding a Port, page 29-17](#)
- [Deleting a Port, page 29-18](#)
- [Changing Port Settings, page 29-18](#)
- [Viewing the Port Certificate, page 29-20](#)

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 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 click Port . |
|---------------|---|

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

Step 3 On the New Port page, enter the applicable settings and click **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, click **Check Telephony Configuration** and click **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 click **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 Click **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 click **Port**.

Step 2 On the Search Ports page, click 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 click **Save**.

Depending on the phone system integration, some or all of the fields in [Table 29-3](#) appear.

Table 29-3 Port Basics Page Settings

Field	Considerations
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not answered. Typically, the port is disabled only by the installer during testing.
Server Name <i>(not available for PIMG/TIMG integrations)</i>	<i>(For Cisco Unity Connection redundancy only)</i> Click the name of the Cisco Unity Connection server that you want to handle this port. Assign an equal number of answering and dial-out voice messaging ports to the Connection servers so that they equally share the voice messaging traffic.
Extension <i>(available for PIMG/TIMG integrations only)</i>	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 <i>(not used by serial integrations)</i>	Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports. 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 <i>(not available for SIP integrations)</i>	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, Connection uses the port that has been idle the longest.
Security Mode <i>(available for Cisco Unified CM SCCP integrations only)</i>	Click the applicable security mode: <ul style="list-style-type: none"> • 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. • 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. • 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, click **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, click **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 click **Port**.
- Step 2** On the Search Ports page, click the display name of the voice messaging port for which you want to see the device certificate.
- Step 3** On the Port Basics page, click **View Certificate**.
- Step 4** In the View Port Certificate window, the information from the port device certificate is displayed.
-

Managing Phone System Trunks

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 29-21](#)
- [Deleting a Phone System Trunk, page 29-21](#)
- [Changing Phone System Trunk Settings, page 29-21](#)

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 click **Trunk**.
 - Step 2** On the Search Phone System Trunks page, under Phone System Trunk Search Results, click **Add New**.
 - Step 3** On the New Phone System Trunk page, enter the applicable settings and click **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 click **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** Click **Delete Selected**.
 - Step 4** When prompted to confirm that you want to delete the phone system trunk, click **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 click 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 | Click Delete Selected . |
| Step 4 | When prompted to confirm that you want to delete the phone system trunk, click OK . |
| Step 5 | Click Add New . |
| Step 6 | On the New Phone System Trunk page, enter the applicable settings and click Save . |
-

Security (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 29-22](#)
- [Saving the Cisco Unity Connection Root Certificate as a File, page 29-23](#)
- [Adding a SIP Certificate \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-23](#)
- [Deleting a SIP Certificate \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-24](#)
- [Changing a SIP Certificate \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-24](#)
- [Adding a SIP Security Profile \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-25](#)
- [Deleting a SIP Security Profile \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-25](#)
- [Changing a SIP Security Profile \(Cisco Unified Communications Manager SIP Trunk Integrations Only\), page 29-25](#)

Viewing the Cisco Unity Connection Root Certificate

Revised May 2009

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 click **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

Revised May 2009

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 click **Root Certificate**.
- Step 2** On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and click **Save Target As**.
- Step 3** In the Save As dialog box, browse to the location where you want to save the Connection root certificate as a file.
- Step 4** In the File Name field, confirm that the file name 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** Click **Save**.
- Step 6** In the Download Complete dialog box, click **Close**.
- Step 7** The 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)

Revised May 2009

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 click **SIP Certificate**.
 - Step 2** On the Search SIP Certificates page, click **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** Click **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 click **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** Click **Delete Selected**.
 - Step 4** When prompted to confirm that you want to delete the SIP certificate, click **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 click **SIP Certificate**.

- Step 2** On the Search SIP Certificates page, click the name of the SIP certificate that you want to change.
 - Step 3** On the Edit SIP Certificate page, enter the applicable settings and click **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 click **SIP Security Profile**.
 - Step 2** On the Search SIP Security Profiles page, click **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** Click **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 click **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** Click **Delete Selected**.
 - Step 4** When prompted to confirm that you want to delete the SIP security profile, click **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 click **SIP Security Profile**.
- Step 2** On the Search SIP Certificates page, click 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 click **Save**.
-



CHAPTER 30

Creating a Cisco Unified Mobility Advantage Integration

See the following sections:

- [About the Cisco Unified Mobility Advantage Integration, page 30-1](#)
- [Task List for Creating an Integration with Cisco Unified Mobility Advantage, page 30-1](#)
- [Requirements, page 30-2](#)
- [Configuring Cisco Unity Connection, page 30-2](#)
- [Testing the Integration with Cisco Unified Mobility Advantage, page 30-3](#)

About the Cisco Unified Mobility Advantage Integration

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 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 30-2](#).
2. Configure Cisco Unified Mobility Advantage. Refer to 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. Refer to *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](#)” section on [page 30-2](#).
5. Test the integration with Cisco Unified Mobility Advantage. See the “[Testing the Integration with Cisco Unified Mobility Advantage](#)” section on [page 30-3](#).

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 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

Configuring Cisco Unity Connection

Do the following procedure.

To Configure Cisco Unity Connection

-
- Step 1** Log on to Cisco Unity Connection Administration as a user that is assigned to the Remote Administration role.
 - Step 2** Expand **Class of Service**, then click **Class of Service**.
 - Step 3** On the Search Class of Service page, click the class of service for the Cisco Unified Mobile Communicator end users who will have access to voice messages in Connection.
 - Step 4** On the Edit Class of Service page, under Licensed Features, check the **Allow Users to Access Voice Mail Using an IMAP Client** check box and click 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** Click **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 Connection.
-

Testing the Integration 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. |
-



CHAPTER 31

Setting Up Phone View

Revised May 2009

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:

- *System Requirements for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.
- *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcumbesysreqs.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 31-2
 - [To Configure Cisco Unified Communications Manager for Phone View \(Cisco Unified CM 5.x\)](#), page 31-2
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 31-3.
3. Enable Phone View for users. See the “[Phone View](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 6.x and Later)

-
- Step 1** In Cisco Unified CM Administration, click **User Management > Application User**.
- Step 2** On the Find and List Application Users page, click **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:
- In the User ID field, enter a unique name for the application user. For example, enter "PhoneViewUser."
 - In the password field, enter a password for the application user.
 - In the Confirm Password field, re-enter the password that you entered in [Step 3b](#).
 - Under Device Information, to the right of the Available Devices field, click **Find More Phones**.
 - On the Find and List Phones page, select the phones on which you want to enable Phone View and click **Add Selected**.
 - 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 click the **Down** arrow below the field to move the phones to the Controlled Devices field.
 - Under Permissions Information, click **Add to User Group**.
 - On the Find and List User Groups page, check the **Standard CCM Admin Users** check box and click **Add Selected**.
 - On the Application User Configuration page, click **Save**.
 - Under Application User Information, click **Edit Credential**.
 - On the Credential Configuration page, confirm that the **User Must Change at Next Login** check box is not checked and click **Save**.
- Step 4** Continue with the ["To Enable Phone View for a Phone System \(Cisco Unified Communications Manager Only\)"](#) section on page 31-3.
-

To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 5.x)

-
- Step 1** In Cisco Unified Communications Manager Administration, click **User Management > Application User**.
- Step 2** On the Find and List Application Users page, click **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:
- In the User ID field, enter the name of the a unique name for the application user. For example, enter "PhoneViewUser."
 - In the password field, enter a password for the application user.
 - In the Confirm Password field, re-enter the password that you entered in [Step 3b](#).
 - Under Device Information, to the right of the Available Devices field, click **Find More Phones**.

- e. On the Find and List Phones page, select the phones on which you want to enable Phone View and click **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 click the **Down** arrow below the field to move the phones to the Controlled Devices field.
- g. On the Application User Configuration page, click **Save**.
- h. Click **User Management > User Group**.
- i. On the Find and List User Groups, click **Standard CCM Admin Users**.
- j. On the User Group Configuration page, click **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 3g](#).
- l. Click **Add Selected**.

Step 4 Continue with the [“To Enable Phone View for a Phone System \(Cisco Unified Communications Manager Only\)”](#) section on page 31-3.

To Enable Phone View for a Phone System (Cisco Unified Communications Manager Only)

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **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 user name is case-sensitive.
 - Step 5** In the CTI Phone Access Password field, enter the password for the application user.
 - Step 6** Click **Save**.
-



CHAPTER 32

Creating a Cisco Fax Server Integration

See the following sections:

- [About the Cisco Fax Server Integration, page 32-1](#)
- [Task List for Creating a Cisco Fax Server Integration, page 32-2](#)
- [Requirements, page 32-2](#)
- [Configuring the Cisco Fax Server, page 32-2](#)
- [Configuring Cisco Unity Connection, page 32-5](#)
- [Configuring Users, page 32-7](#)
- [Testing the Cisco Fax Server Integration, page 32-7](#)
- [Changing the Cisco Unity Connection Configuration for the Cisco Fax Server Integration, page 32-8](#)
- [Changing the User Configuration for the Cisco Fax Server Integration, page 32-9](#)
- [Configuring a Single Number to Receive Both Voice Calls and Faxes, page 32-9](#)

About the Cisco Fax Server Integration

Revised May 2009

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 Cisco Unity 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 Connection server. The Text to Speech (TTS) feature cannot read faxes.

Note that 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

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 32-2.
2. Configure the Cisco Fax Server. See the “Configuring the Cisco Fax Server” section on page 32-2.
3. Configure Cisco Unity Connection. See the “Configuring Cisco Unity Connection” section on page 32-5.
4. Configure the Connection user accounts. See the “Configuring Users” section on page 32-7.
5. Test the Cisco Fax Server integration. See the “Testing the Cisco Fax Server Integration” section on page 32-7.



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 Configuration for the Cisco Fax Server Integration” section on page 32-8 and the “Changing the User Configuration for the Cisco Fax Server Integration” section on page 32-9.

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 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

Configuring the Cisco Fax Server

Revised May 2010

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 log on to the Cisco Fax Server, on the Start menu, click **All Programs > RightFax Enterprise Fax Manager**.
- Step 2** In the left pane of the RightFax Enterprise Fax Manager window, click 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 click **Configure Services**.
- Step 5** Click the **eTransport** tab.
- Step 6** In the SMTP Hostname field, enter the IP address of the Connection server.
- Step 7** Click 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, 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, Connection notifies the user of the successful fax.
- Step 10** Click **OK**.
-

To Set Up the Windows Email Service for POP3

- Step 1** On the Cisco Fax Server, on the Windows Start menu, click **Control Panel > Add or Remove Programs**.
- Step 2** In the Add or Remove Programs window, in the left pane, click **Add/Remove Windows Components**.
- Step 3** In the Windows Components wizard, on the Windows Components page, check the **E-mail Services** check box and click **Next**.

- Step 4** On the Completing the Windows components Wizard page, click **Finish**.
- Step 5** Close the Add or Remove Programs window.
- Step 6** On the Windows Start menu, click **All Programs > Administrative Tools > POP3 Service**.
- Step 7** In the POP3 Service window, in the left pane, expand the Cisco Fax Server and click the Cisco Fax Server node.
- Step 8** In the right pane, click **Add Mailbox**.

**Caution**

A domain for the POP3 mailbox 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 32-4](#).

- Step 11** In the Confirm Password field, re-enter the password and click **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 click **Configure Service**.
- Step 3** In the E-mail configuration dialog box, click **Add Gateway**.
- Step 4** In the E-mail Gateway Selection dialog box, click **SMTP/POP3** and click **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 32-3](#).
- 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** Click **OK**.

To Configure IIS Relay for the POP3 Mailbox on the Cisco Fax Server

- Step 1** On the Windows Start menu, click **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 click **Properties**.
 - Step 3** In the Default SMTP Virtual Server Properties dialog box, click the **Access** tab.
 - Step 4** Under Relay Restrictions, click **Relay**.
 - Step 5** In the Relay Restrictions dialog box, confirm that **Only the List Below** is selected.
 - Step 6** Under Computers, click **Add**.
 - Step 7** In the Computer dialog box, click Single Computer and enter the IP address of the Cisco Fax Server.
 - Step 8** Click **OK**.
 - Step 9** In the Relay Restrictions dialog box, click **OK**.
 - Step 10** In the Default SMTP Virtual Server Properties dialog box, click **OK**.
 - Step 11** Close the Internet Information Services (IIS) Manager window.
-

To Add Connection Users to the Cisco Fax Server

- Step 1** In the RightFax Enterprise Fax Manager window, in the right pane, right-click **Users** and click **New**.
 - Step 2** In the User Edit dialog box, in the User ID field, enter the alias for the Connection user.
 - Step 3** In the User Name field, enter the name of the Connection user.
 - Step 4** In the Group ID field, confirm that **Everyone** is selected.
 - Step 5** In the Voice Mail Subscriber ID field, enter the extension for the Connection user.
 - Step 6** In the E-mail Address field, enter <Connection user alias>@<fully qualified DNS name of the Connection server>.
 - Step 7** Click the **Inbound Routing** tab.
 - Step 8** In the Routing Code (DID/DNIS Number) field, enter the extension of the Connection user.
 - Step 9** In the Routing Type field, click **SMTP**.
 - Step 10** Click the **Notification** tab.
 - Step 11** In the Method field, click **SMTP**.
 - Step 12** In the Notification Address/Info field, enter <Connection user alias>@<Connection server name>.
 - Step 13** Click **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

Revised May 2010

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 click **SMTP Configuration > Server**.
 - Step 2** On the SMTP Server Configuration page, in the Edit menu, click **Search IP Address Access List**.
 - Step 3** On the Search IP Address Access List page, click **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** Click **Save**.
 - Step 6** Check the **Allow Connection** check box and click **Save**.
-

To Enable the Cisco Fax Server Integration on Cisco Unity Connection

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **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** Click **Save**.
-

To Customize the Cisco Fax Server Integration on Cisco Unity Connection

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Advanced > Fax**.
 - Step 2** In the Fax Configuration page, in the Faxable File Types field, enter the file extensions (separated by a comma) that Connection keeps in messages that are delivered to the Cisco Fax Server. 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 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 Connection detects this prefix, it generates a non-delivery receipt and places it in the user mailbox.

Step 5 Click **Save**.

Configuring Users

Do the following procedure.



Note

The Cisco Fax Server must have a subscriber for each 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 click **Users**.

Step 2 On the Search Users page, click 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 click **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, click the name of the Cisco Fax Server.

Step 5 Click **Save**.

Step 6 Repeat [Step 2](#) through [Step 5](#) for all remaining users.



Note

You can use the Bulk Edit Utility to add or change fax extensions for multiple users at once.

Testing the Cisco Fax Server Integration

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 Log on 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 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 click **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** Click **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 click **Advanced > Fax**.
- Step 2** In the Fax Configuration page, in the Faxable File Types field, enter the file extensions (separated by a comma) that Connection keeps in messages that are delivered to the Cisco Fax Server. 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 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 Connection detects this prefix, it generates a non-delivery receipt and places it in the user mailbox.
- Step 5** Click **Save**.
-

Changing the 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 click **Users**.

Step 2 On the Search Users page, click 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 click **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, click the name of the Cisco Fax Server.

Step 5 Click **Save**.

Step 6 Repeat [Step 2](#) through [Step 5](#) for all remaining users.

**Note**

You can use the Bulk Edit Utility to change fax extensions for multiple users at once.

Configuring a Single Number to Receive Both Voice Calls and Faxes

Added May 2009

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 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/web/psa/products/index.html>.

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/web/psa/products/index.html>.

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 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.
- The TCL script file `app_fax_detect.2.1.2.3.tcl` or later.



CHAPTER 33

Using Digital Networking

Each Cisco Unity Connection server (or cluster) has a maximum number of users that it can serve. When the messaging needs of your organization require more than one Connection system, the systems can be networked together such that they replicate directory information among all the systems on the Connection Digital Network.

Users can send, reply to, and forward messages or place calls to users on other Connection systems as though they share the same system, while at the same time, each Connection installation in the network continues to serve only those users that were created on the server or cluster.

Users use the same Connection tools for messaging with users on other networked Connection systems that they use for messaging with users on their home system. Because of directory replication, each Connection system has the information that it needs to address messages to users who are associated with the other Connection systems.

When Connection servers are digitally networked, cross-server features can also be configured such that:

- Calls are transferred to users who are not associated with the local server, according to the call transfer and screening settings of the user who receives the transfer. (This includes calls that are transferred from the automated attendant or directory assistance, and live reply calls that are transferred when a user listens to a message and chooses to reply by calling the sender.)
- When calling from outside the organization to log on to Connection, all users can call the same number regardless of which Connection server they are homed on, and they are transferred to the applicable home Connection server to log on.

In this chapter, you will find procedures for setting up and using Digital Networking, followed by detailed discussions of the concepts and terminology that you need to understand. See the following sections:

- [Setting Up Cisco Unity Connection to Use Digital Networking, page 33-2](#)
- [Procedures for Setting Up Cisco Unity Connection to Use Digital Networking, page 33-3](#)
- [Manually Synchronizing Locations, page 33-17](#)
- [Removing a Location From the Network](#)
- [Digital Networking Concepts and Definitions, page 33-19](#)
- [Notable Behavior, page 33-24](#)



Note

The Cisco Unity Connection Digital Networking feature is not supported in Cisco Unified Communications Manager Business Edition (CMBE).

Setting Up Cisco Unity Connection to Use Digital Networking

This section describes the prerequisites for setting up Digital Networking, and provides a high-level task list of all of the tasks that you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with Digital Networking, you should first read the “[Digital Networking Concepts and Definitions](#)” section on page 33-19 and then review the task list and procedures before beginning the setup.

Prerequisites

Revised May 2009

Before starting the setup, verify that the following prerequisites have been met on each server that will join the Digital Network (for clusters, verify these prerequisites for the publisher server):

- The server meets the requirements listed in the “Requirements for Digital Networking” section of the *System Requirements for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.
- Cisco Unity Connection is already installed in a standalone configuration.
- The servers that will be networked together are directly accessible through TCP/IP port 25 (SMTP), or SMTP messages are routable through an SMTP smart host.
- For Connection clusters, you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

In addition, before setting up Digital Networking, you should be familiar with the concepts in the “[Managing Partitions and Search Spaces](#)” chapter.

Task List

Revised May 2009

Use this task list to set up Digital Networking between Cisco Unity Connection systems. The cross-references take you to detailed procedures.

If you have a Connection cluster, do the tasks only on the publisher server.

1. Make decisions about your networking deployment approach and gather information needed to configure Digital Networking. See the “[Making Deployment Decisions and Gathering Needed Information](#)” section on page 33-4.
2. Check the display name of each server that you are joining to the network, and modify it if it is not unique, or if you want to choose a more descriptive name. Also check the SMTP domain of each server that you are joining to the network, and modify it if it is not unique. See the “[Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain](#)” section on page 33-5.



Caution

If the display name of a server matches the display name of another server on the Digital Network, the server will not be able to join the Digital Network. Likewise, if the SMTP domain matches the SMTP domain of another server on the network, the server will not be able to join the Digital Network.

3. If you are setting up Digital Networking for the first time, start by networking two Connection systems together. See the [“Joining Two Cisco Unity Connection Servers to Create a Digital Network”](#) section on page 33-6.
4. To add additional Connection servers to the network, see the [“Adding a Cisco Unity Connection Server to an Existing Network”](#) section on page 33-8.
5. Verify that replication is complete among locations. See the [“Checking Replication Status”](#) section on page 33-9.
6. If any servers on the network require a smart host to transmit and receive SMTP messages from other servers (for example, because a firewall separates the servers, or because the servers are part of a Connection cluster), configure the smart host, and configure the applicable locations to route through the host. See the [“Configuring a Smart Host”](#) section on page 33-10.

**Note**

For each Connection cluster that you have added to the network, you must configure all other locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down. (You also configure the smart host to resolve the SMTP domain of the cluster to both the publisher and subscriber servers.)

7. For each cluster that you have added to the network, add the IP address of the subscriber server to the SMTP IP access list on every other location on the network; this ensures that other locations can receive message traffic from the subscriber server if the publisher server is down. See the [“Configuring SMTP Access for Cluster Subscriber Servers”](#) section on page 33-11.
8. Configure search spaces at each location to allow users who are homed at the location to reach users at other locations. See the [“Configuring Search Spaces for Digital Networking”](#) section on page 33-12.
9. Secure the Digital Networking setup. See the [“Securing the Digital Networking Setup”](#) section on page 33-13.
10. Optionally, set up cross-server logon and cross-server transfers. See the [“Configuring Cross-Server Logon and Transfers”](#) section on page 33-13.
11. Test the Digital Networking setup. See the [“Testing the Digital Networking Setup”](#) section on page 33-14.
12. Optionally, set up a network-wide All Users distribution list. See the [“Creating a Network-Wide All Voice Mail Users Distribution List”](#) section on page 33-16.
13. If any servers on the Digital Network were previously configured as VPIM locations on other servers in the network, clean up the unused VPIM locations. See the [“Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts”](#) section on page 33-17.
14. If you have not already done so, set up VPIM Networking to connect the Connection locations to any other VPIM-compatible voice messaging systems. See the [“Setting Up Cisco Unity Connection to Use VPIM Networking”](#) section on page 34-1.

Procedures for Setting Up Cisco Unity Connection to Use Digital Networking

See the following sections:

- [Making Deployment Decisions and Gathering Needed Information](#), page 33-4

- [Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain, page 33-5](#)
- [Joining Two Cisco Unity Connection Servers to Create a Digital Network, page 33-6](#)
- [Adding a Cisco Unity Connection Server to an Existing Network, page 33-8](#)
- [Checking Replication Status, page 33-9](#)
- [Configuring a Smart Host, page 33-10](#)
- [Configuring SMTP Access for Cluster Subscriber Servers, page 33-11](#)
- [Configuring Search Spaces for Digital Networking, page 33-12](#)
- [Securing the Digital Networking Setup, page 33-13](#)
- [Configuring Cross-Server Logon and Transfers, page 33-13](#)
- [Testing the Digital Networking Setup, page 33-14](#)
- [Creating a Network-Wide All Voice Mail Users Distribution List, page 33-16](#)
- [Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts, page 33-17](#)

Making Deployment Decisions and Gathering Needed Information

Revised May 2009

Before you begin setting up Digital Networking, be sure to plan for the following, and gather the applicable information:

- If your network includes voice messaging servers that do not meet the prerequisites for Digital Networking but support the Voice Profile for Internet Mail (VPIM) protocol (for example, Cisco Unified Communications Manager Business Edition, Cisco Unity Connection 2.x servers, Cisco Unity 4.0 and later, or other VPIM-compatible systems), use VPIM Networking to connect them.

We recommend the following approaches:

- Unless your servers are already configured for VPIM, set up Digital Networking first, then set up VPIM Networking.
- Choose a single Connection location on the Digital Network to handle the configuration of VPIM locations and contacts. This location is referred to as the “bridgehead.” The VPIM location and contact objects are replicated from the bridgehead to all digitally networked Connection locations so that those locations can address VPIM messages; the networked locations then forward the messages to the bridgehead for delivery to the remote voice messaging server. Managing these objects from a single location simplifies maintenance tasks and avoids potential overlaps in contact information that could cause confusion to users when they attempt to address messages.
- If you have already configured VPIM locations on multiple systems that are joining a Digital Network, delete duplicate VPIM locations from all but one server before setting up Digital Networking. For instructions, see the [“Removing a VPIM Location”](#) section on page 34-15.
- If you are migrating a VPIM location to Digital Networking (for example, because you used VPIM Networking to connect two or more Cisco Unity Connection 2.x servers and have upgraded the servers to Connection 7.x and Digital Networking) set up Digital Networking first. After the directory is fully replicated and you have tested message exchange between the Connection locations, remove the VPIM locations and VPIM contacts that represent the migrated servers and their users. The task list reminds you when to do this task.

- By default, every Connection server includes several predefined system distribution lists, which you can modify but not delete. If you have not renamed these lists so that the list names are unique on each server, or if you have added additional lists whose names are identical across servers, during initial replication each server automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names. (The default lists are All Voice Mail Users, Undeliverable Messages, and All Voicemail-Enabled Contacts.) This can cause confusion when local users try to address to those remote lists.

To solve this problem, you can use one of the following approaches:

- If you want to maintain separate lists on each server, you can modify the name of each list on its home server so that it is unique (for example All Voice Mail Users on <Server Name>) and notify your users of the new list names for each server. If you choose this approach, you should also modify the recorded name of each list to indicate its source.
- Alternatively, after setting up Digital Networking, you can create a master list that includes all users on all networked locations. The task list includes instructions on when and how to do this task.
- If you want to synchronize Connection user data with user data in an LDAP directory, we recommend that you configure Connection for integration with the LDAP directory prior to setting up Digital Networking, to simplify testing and troubleshooting.
- Make note of the following information about each server that is joining the network:
 - The IP address or fully qualified domain name (FQDN) of the server.
 - The user name and password of a user account that is assigned to the System Administrator role.
 - The dial strings that other servers will use to call this server, if cross-server logon or transfer will be configured on other servers to hand off calls to this server.

Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain

Revised May 2009

Each Cisco Unity Connection server that you join to a Digital Network must have a unique display name. If the display name is not unique, the server will not be able to join the Digital Network. For new Connection installations, the display name is typically the same as the host name of the server; however, if you changed the display name or upgraded the server from Connection 2.x (which uses “Local VMS” as the default display name), you may need to change the display name so that it does not overlap with other servers on the network.



Tip

Choose a display name for each server that is descriptive and that will help you identify the location when it is listed among all locations in the Digital Network in Cisco Unity Connection Administration.

Each Connection server that you join to the Digital Network must also have a unique SMTP domain. By default, the SMTP domain is configured during installation to include the hostname of the server, in order to insure that it is unique. However, if the SMTP domains of multiple servers have been modified to the same value, you must change the domains to unique values before joining the servers in a Digital Network.

To Verify That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain

-
- Step 1** To check the display name, in Cisco Unity Connection Administration on the first server, expand **Networking**, then click **Connection Locations**.
- Step 2** On the Search Connection Locations page, if the Display Name of the local server is “Local VMS” or matches the display name of another server, or if you want to modify it to choose a more descriptive name, continue with [Step 3](#).
- If the Display Name value appears to be unique and you do not want to change it, skip to [Step 5](#).
- Step 3** Click the Display Name to edit it.
- Step 4** On the Edit Connection Location page, modify the Display Name value, and click **Save**.
- Step 5** To check the SMTP domain, expand **System Settings > SMTP Configuration**, then click **Server**.
- Step 6** On the SMTP Server Configuration page, if the SMTP Domain of the server matches the SMTP Domain of another server, continue with [Step 7](#).
- If the SMTP Domain appears to be unique, skip to [Step 9](#).
- Step 7** Click **Change SMTP Domain**, change the value of the SMTP Domain field, and click **Save**.
- Step 8** Click **OK** to confirm the change.
- Step 9** Repeat [Step 2](#) through [Step 8](#) for each remaining Connection server that will be joined to the Digital Network.
-

Joining Two Cisco Unity Connection Servers to Create a Digital Network

This section contains two procedures. We recommend that you start by doing the first procedure; if Cisco Unity Connection Administration does not indicate that the servers have successfully joined the network in the first procedure, do the second procedure.

- [To Automatically Join Two Cisco Unity Connection Servers, page 33-6](#)
- [To Manually Join Two Cisco Unity Connection Servers, page 33-7](#)

To Automatically Join Two Cisco Unity Connection Servers

-
- Step 1** In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**.
- Step 2** Click **Join Connection Network**.
- Step 3** On the Join Connection Network page, click **Automatically Join the Network**.
- Step 4** In the Remote Location field, enter the IP address or fully-qualified domain name (FQDN) of the Connection server to connect to in order to join the server to the network.
- Step 5** In the Remote User Name field, enter the user name of an administrator at the location specified in the Remote Location field. The administrator user account must be assigned to the System Administrator role.
- Step 6** In the Remote Password field, enter the password for the administrator specified in the Remote User Name field.
- Step 7** Click **Auto Join Network**.

- Step 8** When prompted, click **OK** to confirm. If the status message indicates that you have successfully joined the network and need to activate and start the Connection Digital Networking Replication Agent, continue with [Step 9](#). Otherwise, skip the rest of this procedure and continue with the “[To Manually Join Two Cisco Unity Connection Servers](#)” procedure on page 33-7.
- Step 9** On either server, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.
- Step 10** In the Server list, click the Connection server, and click **Go**.
- Step 11** Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.
- Step 12** Repeat [Step 9](#) through [Step 11](#) on the other server.
-

To Manually Join Two Cisco Unity Connection Servers

- Step 1** In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**. (This server is referred to as the first server for the remainder of the procedure, and the other server is referred to as the second server.)
- Step 2** Click **Join Connection Network**.
- Step 3** On the Join Connection Network page, click **Manually Join the Network**.
- Step 4** Click **Download** and save the first server configuration file to a location on your hard drive, or on media that you can use to copy the file to the second server.
- Step 5** Browse to Connection Administration on the second server.
- Step 6** In Connection Administration on the second server, expand **Networking**, then click **Connection Locations**.
- Step 7** Click **Join Connection Network**.
- Step 8** On the Join Connection Network page, click **Manually Join the Network**.
- Step 9** In the Select the Remote Configuration File to Upload field, click **Browse** and browse to the copy of the configuration file that you downloaded from the first server in [Step 4](#).
- Step 10** Click **Upload**.
- Step 11** When the upload completes, click **Download**, and save the second server configuration file to a location on your hard drive.
- Step 12** In Connection Administration on the first server, in the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file that you downloaded from the second server in [Step 11](#).
- Step 13** Click **Upload**.
- Step 14** On either server, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.
- Step 15** In the Server list, click the Connection server, and click **Go**.
- Step 16** Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.
- Step 17** Repeat [Step 14](#) through [Step 16](#) on the other server.
-

Adding a Cisco Unity Connection Server to an Existing Network

When you add a Cisco Unity Connection server to an existing Connection network of two or more locations, you join the server to a single location on the network; the server you are adding receives a list of all the other locations on the network, exchanges information with each location, and begins replicating directory information with each location.

This section contains two procedures. We recommend that you start by doing the first procedure; if Cisco Unity Connection Administration does not indicate that the server has successfully joined the network in the first procedure, do the second procedure.

- [To Automatically Join a Cisco Unity Connection Server to a Networked Server, page 33-8](#)
- [To Manually Join a Cisco Unity Connection Server to a Networked Server, page 33-8](#)

To Automatically Join a Cisco Unity Connection Server to a Networked Server

- Step 1** In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**.
- Step 2** Click **Join Connection Network**.
- Step 3** On the Join Connection Network page, click **Automatically Join the Network**.
- Step 4** In the Remote Location field, enter the IP address or fully-qualified domain name (FQDN) of the Connection server to connect to in order to join the server to the network.
- Step 5** In the Remote User Name field, enter the user name of an administrator at the location specified in the Remote Location field. The administrator user account must be assigned to the System Administrator role.
- Step 6** In the Remote Password field, enter the password for the administrator specified in the Remote User Name field.
- Step 7** Click **Auto Join Network**.
- Step 8** When prompted, click **OK** to confirm. If the status message indicates that you have successfully joined the network and need to activate and start the Connection Digital Networking Replication Agent, continue with [Step 9](#). Otherwise, skip the rest of this procedure and continue with the [“To Manually Join a Cisco Unity Connection Server to a Networked Server”](#) procedure on page 33-8.
- Step 9** On the server you just added to the network, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.
- Step 10** In the Server list, choose the Connection server, and click **Go**.
- Step 11** Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.
-

To Manually Join a Cisco Unity Connection Server to a Networked Server

- Step 1** In Cisco Unity Connection Administration on the server that is already joined to the network, expand **Networking**, then click **Connection Locations**.
- Step 2** Click **Join Connection Network**.
- Step 3** On the Join Connection Network page, click **Manually Join the Network**.

- Step 4** If you already have a local copy of the configuration file for the server that is already joined to the network, skip to [Step 5](#).
- If you do not have a local copy of the configuration file, click **Download**, and save the file to a location on your hard drive.
- Step 5** In Cisco Unity Connection Administration on the server that you are adding to the network, expand **Networking**, then click **Connection Locations**.
- Step 6** Click **Join Connection Network**.
- Step 7** On the Join Connection Network page, click **Manually Join the Network**.
- Step 8** In the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file for the server that is already joined to the network.
- Step 9** Click **Upload**.
- Step 10** When the upload completes, click **Download**, and save the configuration file of the server that you are adding to the network to a location on your hard drive.
- Step 11** In Connection Administration on the server that is already joined to the network, in the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file that you downloaded in [Step 10](#).
- Step 12** Click **Upload**.
- Step 13** On the server that you just added to the network, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.
- Step 14** In the Server list, click the Connection server, and click **Go**.
- Step 15** Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.
-

Checking Replication Status

When initial replication begins among locations, it can take a few minutes to a few hours for data to be fully replicated between all locations, depending on the size of your directory.

The Connection Locations pages in Cisco Unity Connection Administration provide information about the status of replication between locations.

To Check Replication Status

- Step 1** In Cisco Unity Connection Administration on a server that is joined to the network, expand **Networking**, then click **Connection Locations**.
- Step 2** On the Search Connection Locations page, in the Locations table, the Push Directory column indicates whether a directory push to the remote location from the location you are accessing is in progress. The Pull Directory column indicates whether a directory pull from the remote location is in progress.
- For example, if an administrator initiates a Push Directory To request from ServerA to ServerB, the Connection Administration on ServerA shows that a directory push to ServerB is in progress, and the Connection Administration on ServerB shows that a directory pull from ServerA is in progress.

**Caution**

Initial replication happens automatically. Do not initiate a directory push or pull while initial replication is in progress.

- Step 3** To get more information about the status of replication with a particular remote location, click the **Display Name** of the remote location.
- Step 4** On the Edit Connection Location page, the Last USN Sent, Last USN Received, and Last USN Acknowledged fields indicate the sequence numbers of replication messages sent to and from the remote location. If the Last USN Sent value is higher than the Last USN Acknowledged value, this location is not currently fully synchronized with the remote location; in this case, the Last USN Acknowledged value should continue to increase periodically. (Note that the Last USN Sent value may also increase periodically.)

Configuring a Smart Host

Revised May 2009

Digital Networking uses SMTP to transmit both directory information and messages between Cisco Unity Connection locations.

If any pair of locations in the Digital Network cannot transmit and receive SMTP messages directly (for example, because a firewall separates the servers), you must configure these locations to route these messages through an SMTP smart host.

In addition, for each Connection cluster that you add to the network, you must configure all other network locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down, and configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. For example, a network has a single smart host and the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a Digital Network, you would join ServerA, ServerB and ServerD together to form the network. Note the following:

- On ServerA, you would configure the Connection locations for ServerB (which represents cluster 1) and ServerD (which represents cluster 2) to route through the smart host.
- On Server B (the cluster 1 publisher), you would configure the Connection location for ServerD (which represents cluster 2) to route through the smart host.
- On ServerD (the cluster 2 publisher), you would configure the Connection location for ServerB (which represents cluster 1) to route through the smart host.
- On the smart host, you would configure the SMTP domain name of cluster 1 to resolve to the IP addresses of both ServerB and ServerC (for example, by using DNS MX records). You would also configure the SMTP domain name of cluster 2 to resolve to both ServerD and ServerE.

Do the following tasks for each server that requires routing to other locations through a smart host:

1. Configure the SMTP smart host to accept messages from the Connection server. If your Digital Network includes Connection clusters, also configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. See the documentation for the SMTP server application that you are using.
2. Configure the Connection server to relay messages to the smart host. See the [“To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host” procedure on page 33-11](#).
3. Configure the Connection server to route messages to the other Connection locations through the smart host. See the [“To Configure the Cisco Unity Connection Server to Route Inter-Location Messages through the Smart Host” procedure on page 33-11](#).

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 click **Smart Host**.
- Step 2** 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** Click **Save**.
-

To Configure the Cisco Unity Connection Server to Route Inter-Location Messages through the Smart Host

-
- Step 1** In Cisco Unity Connection Administration, expand **Networking**, then click **Connection Locations**.
- Step 2** Click the name of a location that requires routing through a smart host.
- Step 3** Check the **Route to This Remote Location Through SMTP Smart Host** check box.
- Step 4** Click **Save**.
- Step 5** Repeat [Step 1](#) through [Step 4](#) for each additional location that requires routing through the smart host.
-

Configuring SMTP Access for Cluster Subscriber Servers

Revised May 2009

When you create a Digital Network that includes a Cisco Unity Connection cluster server pair, you join only the publisher server of the pair to the network. In order for all locations on the network to communicate with the cluster subscriber server in the event that it has Primary status, you must configure all network locations (except for the publisher server that is clustered with the subscriber server) to allow SMTP connections from the subscriber server.

Directory updates are only replicated from the cluster publisher server. SMTP connectivity is needed so that locations can continue to receive user message traffic while the publisher server does not have Primary status. Replication resumes as soon as the publisher server has Primary status again.

For example, a network has the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a Digital Network, you would join ServerA, ServerB and ServerD together to form the network. Note the following:

- On ServerA, you would need to add the IP addresses of both ServerC and ServerE (the two subscriber servers) to the IP access list so that ServerA can communicate with either subscriber server if it has Primary status.
- On ServerB (the cluster 1 publisher), you would add the IP address of ServerE (the cluster 2 subscriber) to the IP access list; and on ServerD (the cluster 2 publisher), you would add the IP address of ServerC (the cluster 1 subscriber) to the IP access list.

To Configure SMTP Access for Cluster Subscriber Servers

-
- Step 1** On a network location, in Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then click **Server**.
- Step 2** On the Edit menu, click **Search IP Address Access List**.
- Step 3** Click **Add New**.
- Step 4** On the New Access IP Address page, enter the IP address of a cluster subscriber server at another location on the network.



Note Do not enter the IP address of the subscriber server on the publisher server that it is paired with.

- Step 5** Click **Save**.
- Step 6** On the Access IP Address page, check the **Allow Connection** check box.
- Step 7** Click **Save**.
- Step 8** Repeat [Step 2](#) through [Step 7](#) for each additional subscriber server on the network (other than the subscriber server that is paired with the server you are configuring).
- Step 9** Repeat [Step 1](#) through [Step 8](#) on each network location.
-

Configuring Search Spaces for Digital Networking

When you initially set up Digital Networking between the servers, users who are homed on one location are not able to address messages to users at other locations, because the users on each location are in separate partitions and use search spaces that do not contain the partitions of users on the other locations. After initial replication completes between the locations, you can reconfigure your search spaces to include partitions that are homed on other servers, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a remote location. (Note that while both partitions and search spaces are replicated between locations, you cannot assign users or other objects to a partition that is homed on another location.)

At a minimum, if you have not made any changes to the default partitions and search spaces on any server, at each location you can add the default partition of each remote Cisco Unity Connection location to the search space that local users are using. For example, in a network of three servers named ServerA, ServerB, and ServerC with no changes to the system defaults, in Cisco Unity Connection Administration on ServerA you would add the “ServerB Partition” and “ServerC Partition” default partitions as members of the “ServerA Search Space” default search space; in Connection Administration on ServerB you would add “ServerA Partition” and “ServerC Partition” to “ServerB Search Space,” and so on.

For instructions on adding partitions to search spaces see the [“Managing Search Spaces” section on page 28-9](#).

Securing the Digital Networking Setup

No user credentials are transmitted as part of Digital Networking communications. However, in order to protect the security of SMTP addresses that are contained in the messages, make sure that any smart hosts that are involved in SMTP message transmission between Connection locations are configured to route messages properly, as it may be possible to extract SMTP addresses from the messages.

Configuring Cross-Server Logon and Transfers

The cross-server logon feature allows users to call the same number regardless of which Cisco Unity Connection server they are homed on, and they are transferred to the applicable home Connection server to log on. If you do not enable cross-server logon, users need to call the phone number of their home Connection server to log on.

The cross-server transfer feature enables calls from the automated attendant or from a directory handler of one Connection location to be transferred to a user on another networked Connection location, according to the call transfer and screening settings of the called user. When you enable cross-server transfers, cross-server live reply is automatically supported for users whose class of service allows live reply to other users. (Cross-server live reply allows users who listen to their messages by phone to reply to a message from a user on another Connection location by calling the user according to the call transfer and screening settings of the called user.) If you do not enable cross-server transfer, call transfers and live replies to users at other Connection locations are performed by using release-to-switch transfers to the Cross-Server Transfer Extension that is configured on the recipient User Basics page. If you do not enable cross-server transfers and you do not configure the Cross-Server Transfer Extension for a user, then callers who attempt to transfer to the user from another location hear the system default greeting and are able to leave a message for the user instead of being transferred.

By default, each Connection server is configured to ignore cross-server hand-off requests. You can enable cross-server logon and cross-server transfer individually between each pair of locations. In addition to enabling the hand-off and configuring a dial string on the originating location, you must configure the receiving location to accept hand-offs. Do the [“To Enable Cross-Server Logon and Transfers Between Cisco Unity Connection Locations” procedure on page 33-14](#).

Search Space Considerations for Cross-Server Logon and Transfers

When setting up cross-server logon, note that Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is trying to log on. 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 Connection finds when searching the partitions in the order in which they appear in the search space. Check the direct routing rules on each location that handles logon calls from remote users to determine the search space that is set by the rule that sends calls to the Attempt Sign-In conversation. If the partitions that contain remote users are not a part of this search space, cross-server logon does not work, even if it is enabled.

Also note that a mismatch between the search space that is applied to the call on the originating location and the search space that is applied on the receiving location can cause problems for cross-server logins and cross-server transfers. A match could be made on the search scope on the originating location that cannot be made on a different search scope on the receiving location. For this reason, we recommend

that you verify that the same search scope is configured on both originating and receiving locations. For example, call routing rules can be used to direct cross-server calls on the receiving location to the appropriate search space based on the cross-server dial string that is used to reach that location.

To Enable Cross-Server Logon and Transfers Between Cisco Unity Connection Locations

-
- Step 1** In Cisco Unity Connection Administration, on a location that handles logon calls from remote users or transfers calls to remote users (the originating location), expand **Networking**, then click **Connection Locations**.
- Step 2** Click the Display Name of a remote location that will accept cross-server logon or transfer hand-offs for users who are homed on that location (the receiving location).
- Step 3** On the Edit Connection Location page for the receiving location, do the following to initiate cross-server hand-offs to this receiving location:
- To enable cross-server logon hand-offs to the remote location, check the **Allow Cross-Server Login to this Remote Location** check box.
 - To enable cross-server transfer hand-offs to the remote location, check the **Allow Cross-Server Transfer to this Remote Location** check box.
 - Enter the dial string that this location will use to call the remote location when performing the hand-off (for example, the pilot number of the home server).



Note You can enter only one dial string for each remote location that receives hand-offs. If the initiating server is configured for multiple phone system integrations, enter a dial string that all phone system integrations can use to reach the remote location.

- Step 4** Repeat [Step 1](#) through [Step 3](#) on the originating location to configure each remote location that accepts cross-server logon or transfer hand-offs from this location.
- Step 5** To configure the originating location to also accept cross-server logon or transfer requests from other locations (as a receiving location), do the following:
- In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **Conversations**.
 - Check the **Respond to Cross-Server Handoff Requests** check box.
- Step 6** Repeat [Step 1](#) through [Step 4](#) on each location that performs cross-server logon and transfer hand-offs (as an originating location).
- Step 7** Repeat [Step 5](#) on each location that receives cross-server hand-offs (as a receiving location).
-

Testing the Digital Networking Setup

To test the Digital Networking setup, create test user accounts or use existing user accounts on each Cisco Unity Connection location. When setting up user accounts in Cisco Unity Connection Administration to be used in the tests, be sure to do the following for each account:

- Record a voice name.
- Record and enable an internal greeting.
- Assign the user to a search space that includes the partitions of remote users.

- On the User Basics page, check the List in Directory check box.
- On the Playback Message Settings page, check the Before Playing Each Message, Play the Sender's Information check box.

Do the following tests to confirm that Digital Networking is functioning properly:

- [To Verify Messaging Between Users on Different Cisco Unity Connection Locations, page 33-15](#)
- [To Verify Call Transfers From the Automated Attendant to Users on Other Cisco Unity Connection Locations, page 33-15](#)
- [To Verify Call Transfers from a Directory Handler to Users on Other Cisco Unity Connection Locations, page 33-15](#)
- [To Verify Identified User Messaging Between Networked Users \(When Identified User Messaging Is Enabled\), page 33-16](#)
- [To Verify Live Reply Between Users on Different Cisco Unity Connection Locations, page 33-16](#)

To Verify Messaging Between Users on Different Cisco Unity Connection Locations

-
- Step 1** Log on to a Cisco Unity Connection location as a user.
- Step 2** Follow the prompts to record and send messages to users who are associated with other Connection locations.
- Step 3** Log on to the applicable Connection location as the recipient user to verify that the message was received.
- Step 4** Repeat [Step 1](#) through [Step 3](#) in the opposite direction.
-

To Verify Call Transfers From the Automated Attendant to Users on Other Cisco Unity Connection Locations

-
- Step 1** From a non-user phone, call the Connection location that has been configured to handle outside callers, and enter the extension of a user who is associated with another Connection location.
- Step 2** Verify that you reach the correct user phone.
-

To Verify Call Transfers from a Directory Handler to Users on Other Cisco Unity Connection Locations

-
- Step 1** From a non-user phone, call the Connection location that has been configured to handle outside callers, and transfer to a directory handler.
- Step 2** Verify that you can find a user who is associated with another Connection location in the phone directory, and that the directory handler transfers the call to the correct user phone.
-

To Verify Identified User Messaging Between Networked Users (When Identified User Messaging Is Enabled)

-
- Step 1** Verify that Connection plays an internal greeting for users who leave messages, by doing the following sub-steps:
- From a user phone, call a user who is associated with another Connection location, and allow the call to be forwarded to Connection.
 - Verify that the internal greeting plays.
 - Leave a test message.
- Step 2** Verify that users are identified when the recipient listens to a message, by doing the following sub-steps:
- Log on to the applicable Connection location as the recipient user and listen to the test message that you recorded in [Step 1](#).
 - Verify that the user conversation announces who the message is from by playing the recorded voice name of the sending user.
 - After listening to the message, verify that the user conversation allows you to reply to the message.
-

To Verify Live Reply Between Users on Different Cisco Unity Connection Locations

-
- Step 1** From a user phone, call a user who is associated with another Connection location, and allow the call to be forwarded to voice mail.
- Step 2** Leave a message.
- Step 3** Log on to the applicable Connection location as the recipient user and listen to the test message that you recorded in [Step 2](#).
- Step 4** After listening to the message, verify that the user conversation allows you to live reply to the message by saying “Call sender” or by using the applicable key presses for the user conversation type. (To find the key presses for a particular conversation, see the “[Cisco Unity Connection Phone Menus and Voice Commands](#)” chapter of the *User Guide for the Cisco Unity Connection Phone Interface*.)
- Step 5** Verify that the live reply call is correctly transferred to the phone of the user who left the message.
-

Creating a Network-Wide All Voice Mail Users Distribution List

If you would like to create a master distribution list that includes all users on all servers, do the following tasks:

- On each location on the Digital Network, rename the All Voice Mail Users list with a unique name (for example All Voice Mail Users on <Server Name>). For instructions, see the “[Modifying System Distribution Lists](#)” section on page 27-3.
- Create a new All Voice Mail Users system distribution list on one location to use as the master list.
- Add the lists from all locations as members of the master list.
- Put all lists except the master list in partitions that do not belong to a search space that users use, so that they cannot address to any list except the master. For example, on each location, create a new partition called Hidden DLs on <Server Name> and put the list homed at that location in that partition. (By default, new partitions are not a member of any search space.)

**Tip**

To avoid having users generate large amounts of voice message traffic by using reply-all to reply to messages sent to the master list, we strongly recommend that you use search spaces to restrict access to the master list to a small subset of users. These users can use a search space that is essentially identical to the search space that other users use, except for the addition of the partition containing the master list.

Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts

After migrating a Cisco Unity Connection server from VPIM Networking to Digital Networking, you should delete the VPIM location for the server on any other servers on the Digital Network that were previously using VPIM Networking to exchange messages with the server. Likewise, you should delete any VPIM locations on the server that represent other Connection locations on the Digital Network. In order to successfully delete the VPIM locations, you must first delete all contacts that are associated with the location.

Note that when you delete the VPIM contacts that represent Connection users, the contacts are removed from distribution lists; consider reviewing and updating distribution list membership on each server to include remote users as applicable. Also consider notifying users that they need to update the membership of any private lists that include contacts on the server being migrated.

For instructions on deleting a VPIM location and the associated VPIM contacts, see the [“Removing a VPIM Location” section on page 34-15](#).

Manually Synchronizing Locations

If you notice that the directory does not seem to be synchronized between two network locations, do the following procedure.

To Check and Manually Synchronize Locations

- Step 1** In Cisco Unity Connection Serviceability on each location, click **Tools > Service Management**. Verify that the Connection Digital Networking Replication Agent service is active on both locations. If it is not active, activate it.

**Tip**

The status message on the Networking > Connection Locations page in Cisco Unity Connection Administration also alerts you if the replication agent is not active.

- Step 2** In Cisco Unity Connection Administration on either location, expand **Networking**, then click **Connection Locations**.
- Step 3** On the Search Connection Locations page, click the Display Name of the other location.
- Step 4** On the Edit Connection Location page, check the values of the Last USN Sent and Last USN Acknowledged fields.

If the Last USN Sent value equals the Last USN Acknowledged value, skip to [Step 5](#).

If the Last USN Sent value is higher than the Last USN Acknowledged value, and the Last USN Acknowledged value is not increasing after a minute or two, do the following:

- a. Return to the Search Connection Locations page.

- b. Check the check box next to the Display Name of the other location.
- c. Click **Push Directory To**.
- d. Wait until replication completes. The Networking > Connection Locations page indicates the status of replication (you must reload the page to update the status).

Step 5 Repeat [Step 2](#) through [Step 4](#) in Cisco Unity Connection Administration on the other location.

Removing a Location From the Network

Revised May 2009

When you remove a location from a Digital Network, it stops replicating directory information with other locations, and all objects that are homed on the server are removed from other locations. Conversely, all objects that are homed on other locations on the network are removed from the server you are removing.

We recommend that you carefully consider the impacts of removing a location from the Digital Network prior to doing so, particularly if you plan to add the location back to the network later. Consider the following impacts:

- Users on the server are removed from distribution lists that are homed on other locations in the Digital Network, and users on other locations are removed from distribution lists that are homed on the server you remove. If you later add the server back into the Digital Network, you need to update distribution list membership on the re-added server to include any remote users, and update distribution list membership on all other locations in the network to include users on the re-added server.
- System call handlers and interview handlers on other locations that are configured to send messages to a user or distribution list that is homed on the server you remove are reconfigured to send messages to the undeliverable messages list of the location. Likewise, system call handlers and interview handlers on the server you remove that are configured to send messages to a user or distribution list that is homed on another location are reconfigured to send messages to the local undeliverable messages list. If you later add the server back into the Digital Network, you need to update the recipients for these handlers to use the correct remote object. (Even if you do not plan to add the server back into the Digital Network, you should make sure that someone is checking messages that are sent to the undeliverable messages list, or reassign handlers that use it as a recipient.)
- Partitions that are homed on the server are removed from search spaces that are homed on other locations in the Digital Network, and partitions that are homed on other locations are removed from search spaces that are homed on the server you remove. A copy is made of search spaces that are homed on the server that are in use by other locations in the Digital Network (and likewise, the server makes a copy of remote search spaces that are homed on other locations). The copies replace the original search spaces on any objects that reference them. If you later add the server back into the Digital Network, you need to update the partition membership of search spaces on the re-added server to include any remote partitions, and update the partition membership of search spaces on all other locations in the network to include partitions on the re-added server.
- On each location in the Digital Network, there are configuration settings specific to other locations (for example, the fields related to cross-server transfers and SMTP routing). When you remove a server from the network, the settings for all locations in the network are deleted from the server that you remove, and the settings for the server that you remove are deleted from all other locations in

the network. If you later add the server back into the Digital Network, you need to update the settings for the re-added server on all other locations in the network, and configure the settings for all other locations on the re-added server.

Do the following procedure to remove a location from the Digital Network. You can remove only one Connection location from the network at a time.

Depending on the size of the directory, removing a Cisco Unity Connection location can take a few minutes to a few hours. Even though the operation may have completed on the local location, it may continue to be in progress on remote locations. We recommend that you wait for the removal operation to complete on all locations in the network before making additional changes to the network.

To Remove a Cisco Unity Connection Location From the Digital Network

-
- Step 1** In Cisco Unity Connection Administration on any location in the Digital Network, expand **Networking**, then click **Connection Locations**.
- Step 2** Check the check box to the left of the Display Name of the location that you want to remove.
- Step 3** Click **Remove Selected**.
- Step 4** Click **OK** to confirm the removal.

**Caution**

Until Connection Administration returns a status message indicating that the removal is complete, avoid making other changes on the Digital Network (for example, removing another location, joining a new location to the network, or initiating a directory push or pull).

Digital Networking Concepts and Definitions

The following sections explain Digital Networking concepts in detail:

- [Cisco Unity Connection Locations and Digital Networking, page 33-19](#)
- [Object Replication, page 33-20](#)
- [Addressing Options for Non-Networked Phone Systems, page 33-21](#)
- [Identified User Messaging Between Networked Cisco Unity Connection Users, page 33-22](#)
- [Cross-Server Logon and Transfers, page 33-23](#)
- [System Distribution Lists, page 33-23](#)
- [Private Distribution Lists, page 33-24](#)
- [VPIM Locations and Digital Networking, page 33-24](#)

Cisco Unity Connection Locations and Digital Networking

Central to how Digital Networking works is an object referred to as a Cisco Unity Connection location. Each Connection server (or cluster) on the network is represented by a single Connection location, which is created locally during installation and which cannot be deleted from the server itself. When you join the server (or cluster) to a Digital Network, a Connection location is created for the server (or cluster) on all other locations in the network, and these locations automatically begin to perform directory

synchronization with the new location. If you remove the server (or cluster) from the Digital Network, the corresponding Connection location is removed from all other locations on the network, and its directory information is automatically removed from these locations (and vice versa). A Connection location can only belong to a single Digital Network. As soon as you join one server to a location on the Digital Network, any other locations on the network are notified of the new location and begin to exchange directory information with the new location.

All objects that you create on a particular location are said to be “homed” on that location. To modify the properties of an object or to delete the object, you must use the administration tools on the location that homes the object. Each location has its own directory of users and other objects, and replicates a subset of these objects and their properties to other locations; the collection of objects and object properties that are replicated among locations is referred to as the Connection directory.

In the context of Digital Networking, an object that is homed on a location is sometimes referred to as local for that location (for example, a local user) and an object that is homed on a different location is referred to as remote.

Object Replication

Each Cisco Unity Connection location replicates the objects and object properties shown in [Table 33-1](#) from its directory to other locations:

Table 33-1 **Replicated Objects in Cisco Unity Connection Digital Networks**

Replicated Object	Replicated Properties
Users with mailboxes	<ul style="list-style-type: none"> • Alias • First name, last name, alternate names • Extension, cross-server transfer extension, and alternate extensions • Partition • Recorded voice name • SMTP proxy addresses
System contacts	All properties
System distribution lists	All properties, including list membership
Partitions	All properties
Search spaces	All properties
Connection location	<ul style="list-style-type: none"> • Display name • Host address • SMTP domain name • Connection version
VPIM locations	All properties except Contact Creation settings (contact creation is handled on the Connection location that homes the VPIM location)

In most cases, you can use replicated objects just as you would use local objects; for example, you can assign a remote user to be the message recipient of a system call handler, or configure the search scope of a user to use a remote search space. Note the following exceptions:

- System call handler owners must be local users.
- Objects that have partition membership (users, contacts, handlers, system distribution lists, and VPIM locations) can only belong to local partitions. You can, however, add a remote partition to a local search space.

When a replicated object that is homed on a Connection location is added, modified or deleted, the location sends an object change request containing details about the change to all other locations. The object change requests for a given location are ordered and tracked with a number known as the Universal Sequence Number (USN). For each change, the location increments the USN by one, and notes the change in its database. When a remote location receives an object change request with a USN value that is one higher than the previous request it received from the sender, it updates its copy of the Connection directory accordingly, and increments its tracked copy of the USN for the sender. If a remote location misses one or more changes and receives a change request with a USN that is more than one higher than the previous request it received from this location, it can request the missed changes by sending the USN values that it missed.

In addition to the USN, each location has another associated number known as the Replication Set. The Replication Set value is used to track the set of changes to which a USN belongs. The Replication Set value is automatically changed during an upgrade, restore, or rollback. This ensures that any changes to the database as a result of the operation are replicated to the network. For example, if Location A receives a message with replication set 10 and USN 5 from Location B, and then receives a message with replication set 9 and USN 5 from Location B, it knows to ignore the message with replication set 9 because it is a lower number and the message predates the message with replication set 10. If Location A receives another message from Location B with replication set 10 and USN 5 again, Location A knows this is a duplicate message and can ignore it.

Addressing Options for Non-Networked Phone Systems

If your organization has a separate phone system for each location, users at one location dial a complete phone number, not just an extension, when calling someone at another location. When users log on to Cisco Unity Connection to send messages to users on another Connection server, the number that they enter when addressing a message by extension depends on whether the Connection numbering plans overlap across locations.

When user extensions on one Connection location overlap with user extensions on another location, you can provide unique extensions for each user by setting up alternate extensions for each user account. For each user, enter a number for the alternate extension that is the same as the full phone number for the user, and make sure the alternate extension is in a partition that is a member of the search spaces that users at other locations use. In this way, when users log on to Connection to send messages, the number they enter when addressing messages is the same number that they use when calling.

When Connection numbering plans do not overlap across locations—that is, when user extensions are unique across locations—users can enter an extension when addressing a message to a user who is associated with another Connection server. As a convenience for users, you may choose to add alternate extensions to each user account, so that users do not need to remember two different numbers—one for calling a user directly, and one for addressing a message. If the numbering plans for each location do not overlap, setting up alternate extensions is optional because they are simply a convenience for users. However, if you do not set up alternate extensions, be sure to tell users to use the extension instead of the full phone number when addressing messages to users who are associated with another location.

Note that alternate extensions have other purposes beyond their use in Digital Networking, such as handling multiple line appearances on user phones. For more information, see the “[Alternate Extensions](#)” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Identified User Messaging Between Networked Cisco Unity Connection Users

When a user calls another user, and the call is forwarded to the greeting of the called user, the ability of Cisco Unity Connection to identify that it is a user who is leaving a message is referred to as identified user messaging. Because Connection is able to identify the caller as a user:

- Connection plays the internal greeting of the called user when the caller leaves a message.
- Connection plays the recorded voice name of the user who left the message when the recipient listens to the message.
- Connection allows the recipient to record a reply.

It is important to note the difference between the following two circumstances:

- A user logs on to Connection, and then records and sends a message. In this circumstance, when the user has logged on to Connection, Connection can identify the message as being from the user, regardless of which Connection server the message recipient is homed on. In this case, the phone system is not involved and the recipient phone does not ring. Instead, the message is sent via Digital Networking.
- A user places a phone call to another user, and then leaves a message. This circumstance is the basis of identified user messaging. As long as identified user messaging is enabled on a Connection location, Connection is able to identify both local and remote users. Note, however, that for identified user messaging to work in both cases, the initial search scope of the call must be set to a search space that locates the correct user based on the calling extension, regardless of whether the caller is a local or remote 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 Connection finds when searching the partitions in the order that they appear in the search space.

In situations where numbering plans overlap across locations, it is therefore possible to have a user leave a message that is incorrectly identified as coming from another user with the same extension in a different partition. Because the initial search scope of the call is based on call routing rules, to avoid this situation, use the following configuration guidelines:

- Maintain a separate search space for each location in which the partition containing its users appears first in the search space. (By default, each Connection server uses its own default partition and default search space, which are replicated to other locations when the server is networked.)
- On each location, set up forwarded call routing rules specific to each other location by specifying a routing rule condition that applies only to calls from the location (for example, based on the port or phone system of the incoming call). Configure the rule to set the search scope of the call to the search space in which the partition containing users at the location appears first.

Cross-Server Logon and Transfers

In order to limit replication traffic and keep the directory size manageable, only a subset of user information is replicated from the home location of the user to other locations on the Digital Network. For this reason, only the user home location has information about call transfer settings, greetings, and other specific details for the user. In order for a Cisco Unity Connection location to properly handle calls destined for a user on a different location, Connection must hand off the call to the home location of the user.

When a Connection location initiates a cross-server logon, cross-server transfer, or cross-server live reply to hand off a call to another location, the hand-off details are negotiated by using DTMF tones, in the following process:

1. The Connection location on which the logon, transfer, or live reply originates puts the caller on hold and calls the home Connection location.
2. When the home location answers, the originating location sends a sequence of DTMF tones that identify the call as a hand-off request.
3. The home location responds with a sequence of DTMF tones, and the originating location hands off the call to the home location for processing along with a DTMF packet that contains the caller ID and the called ID.

At this point the functionality is the same as if the call had originated on the home location.

Systemwide advanced conversation settings allow you to modify the parameters of hand-off calls.

System Distribution Lists

Because system distribution lists are replicated among locations in the network, a user can address messages to any system distribution list at any location, as long as the list is reachable in the user search scope.

When a user addresses a message to a system distribution list, the local Cisco Unity Connection location parses the distribution list membership. The sending location first addresses messages to any VPIM users that are on the distribution list. Next, the sending location checks to see if there are any remote Connection users in the membership; if so, it sends a single message to each location that homes these remote users, addressed to the distribution list (the home locations each parse the message and deliver to their local users). Finally, the sending location checks for local users in the distribution list membership, and delivers the message to each of them.

Connection includes the following predefined system distribution lists: All Voice Mail Users, Undeliverable Messages, and All Voicemail-Enabled Contacts. Each Connection server in your organization has a distinct version of each of these lists. If you have not changed the names of these lists to be unique, during initial replication each server automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names.

By default, the predefined lists on each Connection location have the same recorded voice name, and the All Voice Mail Users and All Voicemail-Enabled Contacts lists have the same extension at each location (the Undeliverable Messages list by default is not assigned an extension, because users do not typically address messages to this list). When setting up Digital Networking, you should consider modifying the recorded voice name of each All Voice Mail Users list and each All Voicemail-Enabled Contacts list; if you do not, users can hear a confusing list of choices when they address messages by name to one of these lists. When users address by extension to a list whose extension overlaps that of another list, they reach the first list that is located when Connection searches the partitions of the user search space in order.

**Tip**

Distribution lists can be nested such that a distribution list contains other lists. You can create one master All Voice Mail Users distribution list that contains the All Voice Mail Users list of each Connection location.

Private Distribution Lists

When creating private lists, users can add members from other locations if allowed by their search scope, in which case the same set of users who are reachable when addressing a message or placing a call can also be added as members of a private list. Private lists are not replicated to other locations; when a user addresses a message to a private list, the home location of the user expands the distribution list and addresses messages to each individual recipient on the list.

Consider notifying users in the event that the following members are inadvertently removed from their lists:

- When you delete a Cisco Unity Connection location, remote users at that location are removed from all private lists.
- When a VPIM contact becomes a Connection user, the contact is removed from all private lists.

VPIM Locations and Digital Networking

When you use the recommended approach of configuring a single Cisco Unity Connection location on the Digital Network as a bridgehead to handle all VPIM locations, the VPIM location data and all contacts at the VPIM location (including automatically created contacts) are replicated to other locations in the network. When a VPIM message is sent to or from a user at another Connection location, the message first passes to the bridgehead, which handles forwarding the message to the destination server.

If necessary to handle your topology, you can check the Route to this Remote Location Through SMTP Smart Host check box on the VPIM location page in Cisco Unity Connection Administration on the bridgehead server. You may need to do this if, for example, a firewall separates the Connection location from the VPIM location. (Note that in order to route to a location through the smart host you must also configure the smart host on the System Settings > SMTP Configuration > Smart Host page in Connection Administration on the bridgehead server.)

Notable Behavior

This section provides information about notable expected behavior associated with Digital Networking. See the following sections:

- [Broadcast Messages, page 33-25](#)
- [Client Access to Digitally Networked Cisco Unity Connection Servers, page 33-25](#)
- [Mapping Users to Cisco Unity Connection Systems, page 33-25](#)
- [Replication During Bulk Operations, page 33-25](#)
- [Replication with Cisco Unity Connection Clusters, page 33-25](#)

Broadcast Messages

Broadcast messages cannot be sent to multiple locations on a Cisco Unity Connection network.

Client Access to Digitally Networked Cisco Unity Connection Servers

Users on each server must access their home server (or cluster) when using the Cisco Personal Communications Assistant (PCA) and IMAP clients. The phone interface is the only client that provides cross-server logon capability.

Mapping Users to Cisco Unity Connection Systems

Each Cisco Unity Connection system handles a distinct group of users. In large organizations, it is possible that more than one Connection system is in use at the same physical location. In this case, you need to determine which user accounts to create on each of the Connection systems (the “home” Connection system for each user), and keep a record of the mapping. This record is needed for the following reasons:

- User phones must forward calls to the Connection system on which the users are homed.
- If user phones have a “Messages” or a speed-dial button that dials the number to access Connection, the buttons must be configured to call the Connection system on which the users are homed.
- If you do not configure cross-server logon, users must dial the Connection system that they are associated with to check their messages; in this case, you need to tell users the correct number to dial when calling into Connection.

To create a record of the mapping, run the Users report on each Connection system. The information in this report includes the user name and primary location. See the [“Generating Reports”](#) chapter for more information.

Replication During Bulk Operations

Replication is paused during bulk operations, and resumes as soon as the operation completes.

Replication with Cisco Unity Connection Clusters

When you create a Digital Network that includes a Cisco Unity Connection cluster server pair, you join only the publisher server of the pair to the network; directory updates made on a cluster subscriber server are replicated only from the cluster publisher server. If the Digital Network is properly configured, messages continue to be sent to and from the cluster even when the subscriber server has Primary status. However, in order to keep the directory current on the publisher server, the secondary server should not have Primary status for an extended period of time.

■ Notable Behavior



CHAPTER 34

Using VPIM Networking

Cisco Unity Connection supports the Voice Profile for Internet Mail (VPIM) protocol, which is an industry standard that allows different voice messaging systems to exchange voice and text messages over the Internet or any TCP/IP network. VPIM is based on the Simple Mail Transfer Protocol (SMTP) and the Multi-Purpose Internet Mail Extension (MIME) protocols.

VPIM Networking can be used for messaging between Cisco Unity Connection 7.x servers, between Connection 7.x servers and Connection 2.x servers, or between Connection 2.x servers and other VPIM-compatible voice messaging systems such as Cisco Unity 4.0 and later. Note that additional server discovery and directory synchronization functionality is available when you use Digital Networking rather than VPIM to connect multiple Connection 7.x servers; for details, see the [“Using Digital Networking”](#) chapter.

VPIM Networking is a licensed feature. If your organization has multiple Connection servers, each server needs to be licensed and configured for VPIM Networking. For more information on obtaining licenses for Connection features, see the [“Managing Licenses”](#) chapter.

See the following sections:

- [Setting Up Cisco Unity Connection to Use VPIM Networking, page 34-1](#)
- [Procedures for Setting Up Cisco Unity Connection to Use VPIM Networking, page 34-3](#)
- [Deleting VPIM Contacts, page 34-14](#)
- [Removing a VPIM Location, page 34-15](#)
- [VPIM Concepts, page 34-15](#)

Setting Up Cisco Unity Connection to Use VPIM Networking

This section describes the prerequisites for setting up VPIM Networking, and provides a task list containing a high-level view of all of the tasks you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with VPIM Networking, you should first read the [“VPIM Concepts”](#) section on page 34-15 and then review the task list and procedures before beginning the setup.

See the following sections:

- [Prerequisites, page 34-2](#)
- [Task List: Setting Up Cisco Unity Connection to Use VPIM Networking, page 34-2](#)

Prerequisites

Before starting the setup, verify that the following prerequisites have been met:

- Cisco Unity Connection is already installed and connected to the network.
- The remote voice messaging system that Connection will be networked with is listed in the “Requirements for VPIM Networking” section of the applicable system requirements document: *System Requirements for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsystreqs.html or *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucmbesystreqs.html.
- A license file with a VPIM license has been obtained and installed on each Connection server.

Task List: Setting Up Cisco Unity Connection to Use VPIM Networking

Use the task list that follows to set up VPIM Networking in Cisco Unity Connection. The links take you to detailed procedures for the setup.

1. Make decisions about your numbering plan and gather information needed to configure VPIM Networking. See the “[Making Design Decisions and Gathering Needed Information](#)” section on page 34-3.
2. Determine the domain name that is used for messaging between the remote voice messaging system and Connection. See the “[Determining the Domain Name](#)” section on page 34-4.
3. As applicable, configure DNS files. See the “[Resolving Names with IP Addresses](#)” section on page 34-4.
4. Verify network and SMTP connectivity with the remote voice messaging system. See the “[Verifying Connectivity with the Remote Voice Messaging System](#)” section on page 34-5.
5. Create the VPIM locations for each remote voice messaging system. See the “[Creating VPIM Locations](#)” section on page 34-5.
6. Create VPIM contacts for each VPIM location. See the “[Creating VPIM Contacts](#)” section on page 34-6.
7. Optionally, customize the contact creation settings for each VPIM location. See the “[Customizing VPIM Contact Directory Update Settings](#)” section on page 34-11.
8. Optionally, add an alternate name for each VPIM location. See the “[Adding Alternate Names for Each VPIM Location](#)” section on page 34-13.
9. Set up the remote voice messaging system for VPIM. Precisely how this is done depends on the voice messaging system. However, you need to provide the remote system with information about Connection. See the “[Gathering Information About Cisco Unity Connection to Configure Another Voice Messaging System for VPIM](#)” section on page 34-14.
10. Test the setup to verify that Connection can exchange messages with the remote voice messaging system.

Procedures for Setting Up Cisco Unity Connection to Use VPIM Networking

This section contains all of the procedures necessary to set up Cisco Unity Connection for VPIM Networking. See the following sections:

- [Making Design Decisions and Gathering Needed Information, page 34-3](#)
- [Determining the Domain Name, page 34-4](#)
- [Resolving Names with IP Addresses, page 34-4](#)
- [Verifying Connectivity with the Remote Voice Messaging System, page 34-5](#)
- [Creating VPIM Locations, page 34-5](#)
- [Customizing VPIM Locations, page 34-6](#)
- [Creating VPIM Contacts, page 34-6](#)
- [Customizing VPIM Contact Directory Update Settings, page 34-11](#)
- [Adding Alternate Names for Each VPIM Location, page 34-13](#)
- [Gathering Information About Cisco Unity Connection to Configure Another Voice Messaging System for VPIM, page 34-14](#)

For detailed explanations of VPIM Networking concepts, see the [“VPIM Concepts” section on page 34-15](#).

Making Design Decisions and Gathering Needed Information

Revised May 2009

Before you begin setting up Cisco Unity Connection for VPIM Networking, be sure to plan for the following, and gather the applicable information:

- Review your numbering plan strategy to determine whether you need to enter prefixes on the VPIM location and to determine which numbers to assign as Dial IDs for the VPIM locations. (In Connection 7.0, the Dial ID field was named DTMF Access ID.)

We recommend the following policies:

- Establish a fixed length for Dial IDs and, if possible, a fixed length for extensions.
 - Assign unique Dial IDs. Dial IDs should not be the same as other Dial IDs or extensions.
 - Assign Dial IDs that have at least three digits.
 - Use a different number range for Dial IDs than for extensions. Do not use Dial IDs that conflict with extensions, such as 001 or 002.
 - If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs.
- Review your partition and search space configuration to determine the partition and search scope you use for each VPIM location. For more information, see the [“Search Spaces and VPIM Locations” section on page 28-8](#).
 - Decide for each remote voice messaging system whether to allow Connection to automatically create, modify, and delete VPIM contact records for users on that system, based on information received from incoming VPIM messages. Also decide how to map the source information to VPIM contact display names and extensions.

- Decide for each remote voice messaging system whether to allow Connection users to blind address messages to recipients at the location.
- Make note of the following information about the remote voice messaging system: the mailbox range, the server name, the domain name, and the IP address.

Determining the Domain Name

VPIM messages are addressed in the format <Mailbox Number>@<Domain Name>. In order for messages to be exchanged between the remote voice messaging system and Cisco Unity Connection, you need to decide on the domain name that the remote voice messaging system uses when addressing messages to Connection users. The domain name is configured as follows:

- On the remote voice messaging system, the domain name is configured on the location or node profile that corresponds to Connection. (For additional information, see the documentation for the remote voice messaging system.)
- In the SMTP Domain field, on the System Settings > SMTP Configuration > SMTP Server Configuration page in Cisco Unity Connection Administration.

If the remote voice messaging system location or node profile that corresponds to Connection has already been configured with a domain name, use that domain name in the procedures in this section.

Domain Name Requirements

The domain name uniquely identifies the voice messaging system. When choosing domain names used by Connection and the remote voice messaging system, keep the following in mind:

- Connection and the remote voice messaging system cannot use the same domain name. Each system must use a unique domain name.
- The complete domain name used by Connection cannot be a subset of the domain name used by the remote voice messaging system. For example, if Connection is using the domain name cisco.com, the remote voice messaging system cannot use names like london.cisco.com, paris-cisco.com, or romecisco.com. However, you could use europe.cisco.com for Connection, and then use the names london.cisco.com, paris-cisco.com, and romecisco.com for the remote voice messaging systems.



Caution

Choosing a domain name that does not meet these requirements will result in message delivery failure.

Resolving Names with IP Addresses

VPIM messages are sent over the Internet or any TCP/IP network via SMTP. Therefore, a mechanism for name resolution is required for the remote voice messaging server. The supported method for name resolution is through a Domain Name System (DNS).

You need to know the fully qualified domain name (FQDN) and IP address of the remote voice messaging server. The FQDN is displayed on the System Settings > SMTP Configuration > Server page.

Add a host address resource (A) record and a mail exchange (MX) record in DNS for the remote voice messaging server, if they do not already exist.

For more information about adding A and MX records in DNS, see the documentation for the DNS server.

Verifying Connectivity with the Remote Voice Messaging System

Verify that the servers that handle outgoing and incoming SMTP messages have network connectivity with the remote voice messaging server, and vice versa.

For networking with another voice messaging server, you may need to install and configure an SMTP service or gateway on that server. See the documentation of the other voice messaging system for information on installing the SMTP service or gateway. Before proceeding, verify that the SMTP service or gateway has been installed on the other voice messaging server.

To Verify Network Connectivity with the Remote Voice Messaging Server

-
- Step 1** By using a computer on the same local network segment as the Connection server, open a command prompt window.
- Step 2** Enter **ping <IP address>**, where <IP address> is the IP address of the remote voice messaging server, then press **Enter**.
- If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with [Step 3](#).
- Step 3** Enter **ping <Domain name>** where <Domain name> is the domain name that is used to address messages to the remote voice messaging server. The domain name in this step is the domain name that is entered for the VPIM location in Cisco Unity Connection Administration when setting up VPIM Networking.
- Step 4** If you received a reply when pingging the IP address in [Step 2](#), but no replies when pingging the domain name in [Step 3](#), see the “[Resolving Names with IP Addresses](#)” section on page 34-4. When the problem is resolved, continue with [Step 5](#).
- Step 5** Test network connectivity in the opposite direction. For systems other than Connection, see the documentation for information on how to conduct the test, and continue with [Step 6](#). Note that the remaining steps in this procedure may not exactly match the steps necessary for your system, so you may need to make adjustments.
- Step 6** On the remote server, ping the IP address of the local server that handles incoming SMTP messages.
- If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with [Step 7](#).
- Step 7** On the remote server, ping the domain name, where the domain name is the one that is discussed in the “[Determining the Domain Name](#)” section on page 34-4.
- Step 8** If pingging by domain name fails, see the “[Resolving Names with IP Addresses](#)” section on page 34-4.
-

**Note**

Optionally, you can verify network connectivity by using the “utils network ping” CLI command.

Creating VPIM Locations

Revised May 2010

Create a VPIM location on Cisco Unity Connection for each remote voice messaging system to which users send messages. If Connection will message with a large number of voice messaging systems, you may prefer to configure only a few VPIM locations at this time and proceed with the rest of the setup. After verifying that messaging works correctly between Connection and the voice messaging systems for which VPIM locations have been configured, you can create the rest of the VPIM locations.

To Create VPIM Locations

-
- Step 1** In Cisco Unity Connection Administration, expand **Networking**, then click **VPIM Locations**.
 - Step 2** On the Search VPIM Locations page, click **Add New**.
 - Step 3** On the New VPIM Location page, enter basic settings, as applicable. (For field information, on the Help menu, click **This Page**.)



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

- Step 4** Click **Save**.
 - Step 5** On the Edit VPIM Location page, continue entering applicable settings.
 - Step 6** When you have finished entering settings on the Edit VPIM Location page, click **Save**.
-

Customizing VPIM Locations

Revised May 2010

You can customize a VPIM location by using Cisco Unity Connection Administration for each remote voice messaging system to which users send messages.

To Customize VPIM Locations

-
- Step 1** In Cisco Unity Connection Administration, expand **Networking**, then click **VPIM Locations**.
 - Step 2** On the Search VPIM Locations page, click the display name for the VPIM location that you want to customize.
 - Step 3** On the Edit VPIM Location page, change settings, as applicable. (For field information, on the Help menu, click **This Page**.)
 - Step 4** When you have finished changing settings on the Edit VPIM Location page, click **Save**.
-

Creating VPIM Contacts

You may prefer to create only a few VPIM contacts at this point, for testing purposes, until you verify that Cisco Unity Connection and the remote voice messaging system can successfully exchange messages. After you have confirmed that messaging between Connection and the remote voice messaging system is working correctly, you can finish creating the VPIM contacts. Note that you must first create VPIM locations before creating VPIM contacts, and the VPIM contacts must be created on the same Connection server on which you created the VPIM locations.

You can create VPIM contacts by using the Bulk Administration Tool or by using Cisco Unity Connection Administration. See the following sections:

- [Using the Bulk Administration Tool to Create Multiple VPIM Contacts, page 34-7](#)
- [Correcting CSV Errors, page 34-8](#)
- [Using Cisco Unity Connection Administration to Create VPIM Contacts, page 34-9](#)
- [After Creating VPIM Contacts, page 34-10](#)


Using the Bulk Administration Tool to Create Multiple VPIM Contacts

Revised May 2009

The Bulk Administration Tool (BAT) allows you to create multiple VPIM contacts at the same time by importing contact data from a comma-separated value (CSV) file. CSV is a common text file format for moving data from one data store to another.

Use the following procedure to prepare your CSV file.

To Prepare a CSV File for Creating VPIM Contacts

-
- Step 1** Save the data that you will use to create VPIM Contacts as a CSV file.
- As a best practice, do not include more than 7,500 records in a single CSV file, as you may encounter unexpected results when the Bulk Administration Tool imports the data.
- Step 2** Copy the CSV file to the applicable directory.
- Step 3** Open the CSV file in a spreadsheet application or another application with which you can edit and reorganize the data. Do the following:
- Confirm that the data is separated by commas, and that no tabs, spaces, or semicolons separate the data in the file.
 - If any data includes a space, quotation marks, or commas, contain the characters within quotation marks.
- Step 4** Rearrange the data so that the columns are in the same order as the column headers that you will add in [Step 5](#). The order of the column headers does not matter, though it is good practice to set up your CSV file as indicated here. For example, the columns of data in this sample are sorted so that the alias of the contact is followed by the last name, the first name, the extension, the remote mailbox ID (RemoteMailAddress), and then by VPIM location (DeliveryLocationDisplayName):
- ```
aabade,Abade,Alex,2001,3000,Chicago VMS VPIM Location
kbader,Bader,Kelly,2002,3100,Chicago VMS VPIM Location
tcampbell,Campbell,Terry,2003,3200,Chicago VMS VPIM Location
lcho,Cho,Li,2004,3300,Chicago VMS VPIM Location
```
- 

**Note** The only required column headers for creating system contacts are Alias and Extension. However, in order to create VPIM contacts you must also include columns for the remote mailbox ID and the VPIM location.
- 
- Step 5** Enter the column headers above the first row of data. Column headers must be separated by commas, and spelled as indicated below:
- Alias,LastName,FirstName,Extension,RemoteMailAddress,DeliveryLocationDisplayName

- Step 6** If applicable, add optional column headers to the first row, and the corresponding data that you want to import in the subsequent rows below. As you do so, confirm the following:
- Column headers and data are separated by commas. Note that every row does not have to contain data for optional column headers.
  - Any data that includes a space, quotation marks, or commas is contained within quotation marks.



**Tip** Include a column with the ListInDirectory header and a value of 1 for each contact if you would like users to be able to address messages to VPIM contacts the same way that they address messages to regular Connection users—by extension or by spelling the name of the recipient. For a list of optional column headers, see the “[Required and Optional CSV Fields for System Contacts](#)” table in the “Using the Cisco Unity Connection Bulk Administration Tool” appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

- Step 7** If your CSV file contains columns of data that you do not want to import, delete the columns. Alternatively, you can title one column NOTES. The BAT ignores data beneath any NOTES column header, but it does not support more than one NOTES column in a CSV file.
- Step 8** Confirm that each row contains the appropriate data corresponding to each column header.
- Step 9** Save the file as a CSV file.
- Step 10** Continue with the following “[To Create VPIM Contacts by Using the Bulk Administration Tool](#)” procedure.

---

#### To Create VPIM Contacts by Using the Bulk Administration Tool

---

- Step 1** In Cisco Unity Connection Administration, expand **Tools**, then click **Bulk Administration Tool**.
- Step 2** On the Bulk Administration Tool page, under Select Operation, click **Create**.
- Step 3** Under Select Object Type, click **System Contacts**.
- Step 4** Under Select File, click **Browse**.
- Step 5** In the Choose File dialog box, browse to the directory where you saved the CSV file that you created in the “[To Prepare a CSV File for Creating VPIM Contacts](#)” procedure on page 34-7 and click **Open**.
- Step 6** In the Failed Objects File Name field, enter the path and the name of the file in which you want errors recorded.
- Step 7** Click **Submit**.
- 

## Correcting CSV Errors

The failed objects file contains data that failed to create a VPIM contact. The Bulk Administration Tool reports the first error it detects in a row in a CSV file. When you have corrected that error, the BAT may detect additional errors in the same row when the data is imported again. Thus, you may need to repeat the correction process—running the BAT and correcting an error—several times to find and correct all errors.

The failed objects file contains all the records that failed to create a VPIM contact. You can save the file as a CSV file, and use it when you run the BAT again. Note that each time you run the BAT, the failed objects file is overwritten.

#### To Correct CSV Errors That Occurred When Creating VPIM Contacts

- 
- Step 1** If the Bulk Administration Tool operation results in any failures, you can immediately inspect the failed objects report file by clicking **Download the Failed Objects File**.
- Step 2** Open the file and correct all problems with the data, as indicated by the information in the FailureReason column for each record.
- Step 3** Remove the FailureReason column or change the heading to **JUNK**.
- Step 4** When you have finished modifying the data, save the file as a CSV file with a new name.
- Step 5** Run the BAT again with the CSV file that you saved in [Step 4](#) as the input file.
- Note that each time that you run BAT, the failed objects file is overwritten (unless you specify a new name for the file each time you run the tool).
- Step 6** Repeat this procedure until all VPIM contact accounts are created without error, and then proceed to the [“After Creating VPIM Contacts” section on page 34-10](#).
- 

## Using Cisco Unity Connection Administration to Create VPIM Contacts

You can create VPIM contacts one at a time by using Cisco Unity Connection Administration.

#### To Create VPIM Contacts by Using Cisco Unity Connection Administration

- 
- Step 1** In Cisco Unity Connection Administration, expand **Contacts**, then click **Contacts**.
- Step 2** On the Search Contacts page, on the Contact menu, click **New Contact**.
- Step 3** On the New Contact page, enter the following settings and click **Save**.

**Table 34-1** Settings for the New Contact Page

| Field            | Setting                                                |
|------------------|--------------------------------------------------------|
| Alias            | Enter the alias of the VPIM contact.                   |
| First Name       | Enter the first name of the VPIM contact.              |
| Last Name        | Enter the last name of the VPIM contact.               |
| Display Name     | Enter the display name of the VPIM contact.            |
| Contact Template | Select the template on which to base the VPIM contact. |

- Step 4** On the Edit Contact Basics page, enter the following settings and click **Save**.

**Table 34-2 Settings for the Edit Contact Basics Page**

| Field                                                              | Setting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Voice Name                                                         | Click <b>Play/Record</b> to record a voice name for the VPIM contact.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| List in Directory                                                  | Check this check box to list the VPIM contact in the Connection directory.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Partition                                                          | Select the partition to which the VPIM contact belongs. Partitions are grouped together into search spaces, which are used to define the scope of objects (for example, users and distribution lists) that a user or outside caller can reach while interacting with Connection. A VPIM contact can belong to only one partition. A partition can belong to more than one search space.                                                                                                 |
| Transfer Enabled                                                   | <i>(Optional)</i> Check this check box if you want Connection to transfer incoming calls to a phone number that is associated with the VPIM contact instead of sending a message to the remote mailbox for the VPIM contact.                                                                                                                                                                                                                                                            |
| Transfer Extension                                                 | <i>(Optional)</i> Enter the phone number that the phone system uses to transfer calls to the VPIM contact, including any outdial access codes, if necessary. This field works together with the Transfer Enabled field.                                                                                                                                                                                                                                                                 |
| Delivery Location                                                  | Select the VPIM location for the VPIM contact.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| VPIM Remote Mailbox Number                                         | Enter the mailbox number for the VPIM contact on the remote voice messaging system.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Local Extension                                                    | <p><i>(Optional)</i> For VPIM contacts, you can assign a local extension that fits into the Connection extension numbering scheme. A local extension allows callers to address messages to the VPIM contact by using an extension, rather than having to know the location ID and the remote mailbox number of the contact.</p> <p>In addition, if you set the Transfer Enabled and Transfer Extension fields, callers are able to identify and be transferred to the VPIM contact.</p> |
| Phone Numbers to Call Contact by Using Voice Commands              | <p><i>(Optional)</i> Use the Dialed Work Phone, Dialed Home Phone, and Dialed Mobile Phone fields when you want voice recognition users to be able to call the VPIM contact by specifying a specific phone type for the contact.</p> <p>For dialed phone numbers, include any additional numbers necessary to dial outside calls (for example 9) and for long-distance dialing (for example, 1).</p>                                                                                    |
| Phone Numbers to Identify Contact for Personal Call Transfer Rules | <i>(Optional)</i> Use the Work Phone, Home Phone, Mobile Phone, Other Number 1, and Other Number 2 fields to enter phone numbers that Connection uses when matching the personal call transfer rules of a user against incoming phone calls from system contacts.                                                                                                                                                                                                                       |

**Step 5** Repeat [Step 2](#) through [Step 4](#) for all remaining VPIM contacts that you want to create.

## After Creating VPIM Contacts

After creating VPIM contacts, consider the following:

- It takes a few minutes for the newly-created VPIM contact to be available to receive messages.
- You can make changes to settings for individual VPIM contacts in Cisco Unity Connection Administration.

- When you want to modify unique VPIM contact settings—such as the extension—for multiple contacts at once, you can rerun the Bulk Administration Tool.
- When a VPIM contact no longer needs a Connection account, you can delete the VPIM contact. For details, see the [“Deleting VPIM Contacts” section on page 34-14](#).

## Customizing VPIM Contact Directory Update Settings

In addition to manually creating, modifying, and deleting VPIM contacts, you can configure Cisco Unity Connection to automatically update records in the VPIM contact directory based on information that is contained in incoming VPIM messages. The settings that control whether the creation, modification, and deletion actions occur automatically, and how the incoming information is used to create or modify a record, can be individually configured for each VPIM location. By default, no automatic directory updates occur for any VPIM locations.

Depending on the Contact Creation settings that you choose for each VPIM location, Connection uses information from the header of an incoming VPIM message. If a VPIM message is received from a sender on a VPIM location that is configured to allow automatic VPIM contact creation, and no existing VPIM contact matches the information of the sender, a new VPIM contact record is created, provided that the VPIM message contains:

- A phone number
- A text name
- A domain name
- A recorded voice name (when required, based on the VPIM location configuration)

Additional Contact Creation settings allow you to specify how to map the parsed text name of the VPIM contact to a first name, last name, and display name, and how to map the phone number to an extension.



### Note

Changes to the Map VPIM Contact Extensions setting on the Contact Creation page for a VPIM location affect only VPIM contacts that are created after the setting is saved. VPIM contacts that already existed before the Map VPIM Contact Extensions setting is changed are not automatically updated. You must manually change the extension for each previously existing VPIM contact for that VPIM location.

If a VPIM message is received from a sender on a VPIM location that is configured to allow automatic VPIM contact modification, and an existing VPIM contact matches the sender information, the VPIM contact can be updated. You can choose whether VPIM contact information is updated each time a message is received from a VPIM contact, or only when a message is received from a VPIM contact whose text name has changed since the directory entry was created. You can also decide whether or not to allow an update to the display name when a modification is made.

If a message from a Connection user to a VPIM contact results in a non-delivery receipt (NDR), indicating that the message was undeliverable because the intended recipient does not exist (SMTP 5.1.1), and if the VPIM location is configured to allow automatic VPIM contact deletion, the VPIM contact is deleted.

You can update the VPIM location contact creation settings by using Cisco Unity Connection Administration. See the following sections:

- [Before Configuring VPIM Contact Creation Settings, page 34-12](#)
- [Using Cisco Unity Connection Administration to Configure VPIM Contact Creation Settings, page 34-12](#)

## Before Configuring VPIM Contact Creation Settings

Before configuring the VPIM location contact creation settings, consider the following:

- If you have pre-populated VPIM contacts with specific display names that should not be changed, but want to allow automatic modification of other fields in the contact record, you can choose to keep the Allow VPIM Contact Display Name Updates check box unchecked. In this case, the first name, last name, and spoken name of a contact may be modified during an automatic update. This may result in a mismatch if the spoken name is updated and the display name is not.
- When the Allow VPIM Contacts Without Recorded Voice Names check box is not checked, new VPIM contacts are not created for incoming messages that do not contain an Originator-Spoken-Name attachment. In addition, if automatic modification of VPIM contacts is enabled, and if the sender of an incoming message matches an existing VPIM contact, the VPIM contact is deleted if the attachment is not present in the message.
- When the Allow VPIM Contacts Without Recorded Voice Names check box is checked, and automatic modification of VPIM contacts is enabled, if the sender of an incoming message that does not include an Originator-Spoken-Name attachment matches an existing VPIM contact, the existing recorded voice name is deleted.
- If the phone number in an incoming message cannot be successfully mapped to an extension by using the option selected for the Map VPIM Contact Extensions To field, a VPIM contact is not created for the sender.

## Using Cisco Unity Connection Administration to Configure VPIM Contact Creation Settings

After you create a VPIM location, you can configure the settings that control automatic directory updates for that specific VPIM location by using Cisco Unity Connection Administration.

### To Configure VPIM Contact Creation Settings by Using Cisco Unity Connection Administration

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In Cisco Unity Connection Administration, expand <b>Networking</b> , then click <b>VPIM Locations</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 2</b> | On the Search VPIM Locations page, click the name of the VPIM location for which you want to configure contact creation settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 3</b> | On the Edit VPIM Location page, on the Edit menu, click <b>Contact Creation</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 4</b> | On the Contact Creation page, check the <b>Automatically Create VPIM Contacts</b> check box to enable automatic creation of a VPIM contact record for this location when a VPIM message arrives and the sender does not already have a corresponding VPIM contact record.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 5</b> | If you checked the Automatically Create VPIM Contacts check box in <a href="#">Step 4</a> , in the Contact Template list, select the template on which to base the automatically created contacts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 6</b> | In the Automatically Modify VPIM Contact field, click one of the following to apply to VPIM contacts for this location: <ul style="list-style-type: none"><li>• <b>No Automatic Update of Contacts</b>—The VPIM contact record is not updated with the sender information in a VPIM message when an incoming message has changed sender information.</li><li>• <b>Only When the Text Name Changes</b>—The VPIM contact record is updated only when the text name received in the VPIM message does not match the name of the VPIM contact.</li><li>• <b>With Each VPIM Message</b>—Every incoming VPIM message from a VPIM contact at this location results in an update to the corresponding VPIM contact record.</li></ul> |

- Step 7** Check the **Automatically Delete VPIM Contact** check box to enable automatic deletion of a VPIM contact for this location when a VPIM message is returned as undeliverable.
- Step 8** Check the **Allow VPIM Contact Display Name Updates** check box to enable automatic updates to the VPIM contact display name when an incoming message from this location has a changed display name for the sender.
- Step 9** Check the **Allow VPIM Contacts Without Recorded Voice Names** check box to enable automatic updates for this location to records for VPIM contacts that do not have a recorded voice name.
- Step 10** In the Mapping Text Names field, click one of the following options to indicate how text names in incoming messages from this location are mapped to the display names for automatically created VPIM contact records:
- **Directly to VPIM Contact Display Names**—The display names for VPIM contacts match the corresponding text names.
  - **Custom**—Enter the rule that defines how text names are mapped to display names for VPIM contacts. You can enter the tokens <FN>, <LN>, or <TN> (respectively first name, last name, or text name) in any combination, along with any additional text. Always precede <FN>, <LN>, or <TN> with a space, comma, or semicolon unless it appears at the beginning of the rule. In addition, always follow one of these tokens with a space, comma or semicolon unless it appears at the end of the rule. No additional characters are required at the beginning or end of a rule.
- Step 11** In the Map VPIM Contact Extensions To field, click one of the following settings to indicate how the phone number on incoming messages from this location is mapped to the extension for automatically created VPIM contact records:
- **Phone Number**—Extensions are the same as the phone numbers that are parsed from incoming VPIM messages.
  - **Phone Number - Remote Phone Prefix**—Extensions are formed by removing the remote phone prefix from the beginning of the phone numbers.
  - **Location Dial ID + Phone Number**—Extensions are formed by adding the location Dial ID in front of the phone numbers.
  - **Location Dial ID + Phone Number - Remote Phone Prefix**—Extensions are formed by removing the remote phone prefix from the beginning of the phone number, and adding the location Dial ID in front of the resulting number.
- Step 12** Click **Save**.
- Step 13** On the VPIM Location menu, click **Search VPIM Locations**.
- Step 14** Repeat [Step 2](#) through [Step 13](#) for all remaining VPIM locations.
- 

## Adding Alternate Names for Each VPIM Location

When the Cisco Unity Connection system uses the voice-recognition option, you can also specify alternate names for the display name that you give a VPIM location. Users say the display name when they use voice commands to blind address to a mailbox number at a VPIM location (for example, to address to extension 55 at a VPIM location named Seattle, a user would say “five five at Seattle”) or to address a message to a VPIM contact name at a VPIM location (for example, “Robin Smith in Chicago”). Consider specifying alternate names if the VPIM location display name contains administrative information that users are not likely to know, or if it is not pronounced the way it would be read, as may be the case with acronyms and abbreviations. Also consider adding alternate names if users tend to refer

to a location in multiple ways. For example, if users at one site refer to a location as “Seattle branch” and users at another site refer to the same location as “Seattle office,” you could add both “Seattle branch” and “Seattle office” as alternate names.

#### To Add an Alternate Name for VPIM Locations

- 
- Step 1** In Cisco Unity Connection Administration, expand **Networking**, then click **VPIM Locations**.
  - Step 2** On the Search VPIM Locations page, click the name of the VPIM location for which you want to add an alternate name.
  - Step 3** On the Edit VPIM Location page, on the Edit menu, click **Alternate Names**.
  - Step 4** On the Edit Alternate Names page, in the Display Name field, enter the alternate name you want for the VPIM location, then click **Add New**.
  - Step 5** On the VPIM Location menu, click **Search VPIM Locations**.
  - Step 6** Repeat [Step 2](#) through [Step 5](#) for all remaining VPIM locations for which you want to add alternate names.
- 

## Gathering Information About Cisco Unity Connection to Configure Another Voice Messaging System for VPIM

Configuring another voice messaging system to exchange VPIM messages with Cisco Unity Connection may require the following information:

- The server name and domain name of the SMTP server that handles incoming SMTP messages.
- The Connection phone prefix (if any) and Remote phone prefix (if any) entered on the corresponding VPIM location page.
- The mailbox number range for Connection users.

Incoming VPIM messages must be routed to the SMTP server. When defining a location for Connection on the remote voice messaging system, use the domain name that you entered for the SMTP server.

Connection expects incoming VPIM messages to be formatted as follows:

<ConnectionPhonePrefix+ConnectionUserExtension@PrimaryLocationSMTPDomainName>

These specific properties are configured in Connection, but similar information needs to be configured in the other voice messaging system.

## Deleting VPIM Contacts

#### To Delete VPIM Contacts

- 
- Step 1** In Cisco Unity Connection Administration, expand **Contacts**, then click **Contacts**.
  - Step 2** On the Search Contacts page, check the check boxes next to the VPIM contacts that you want to delete.
  - Step 3** Click **Delete Selected**.

**Step 4** When prompted to confirm the deletion, click **OK**.

---

## Removing a VPIM Location

### Revised May 2009

When you remove a VPIM location, you must remove (or reassign) any contacts and contact templates that use the location before deleting the VPIM location object. Use the following task list to remove a VPIM location.

1. Use the Bulk Administration Tool to export a list of all system contacts. See the “[Exporting System Contacts to a CSV File](#)” section in the “Using the Cisco Unity Connection Bulk Administration Tool” appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.
2. Download the export file, and use a text editor to modify it to contain only the rows in which the DeliveryLocationDisplayName matches the display name of the VPIM location that you are removing. (If you plan to reassign the contacts to a different VPIM location, update the value in the DeliveryLocationDisplayName column.)
3. Use the Bulk Administration Tool to delete the list of contacts you generated in Task 2. See the “[Deleting System Contacts](#)” section in the “Using the Cisco Unity Connection Bulk Administration Tool” appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Alternatively, to reassign the contacts to a different VPIM location, use the Update option. See the “[Updating System Contacts](#)” section in the “Using the Cisco Unity Connection Bulk Administration Tool” appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

4. In Cisco Unity Connection Administration, expand Templates, then click Contact Templates. If a contact template is configured to use the VPIM location as the delivery location, change the delivery location, or delete the template. (You may need to click the display name of each template on the Search Contact Templates page to verify or change the delivery location.)
5. To delete the location, in Connection Administration, expand Networking, then click VPIM Locations. On the Search VPIM Locations page, check the check box next to the display name of the location that you want to delete, then click Delete Selected.

## VPIM Concepts

The following sections explain VPIM concepts in detail:

- [VPIM Messages, page 34-16](#)
- [VPIM Addresses, page 34-17](#)
- [Message Addressing Options, page 34-17](#)
- [Messaging Similarities and Limitations, page 34-17](#)
- [Audio Format Considerations, page 34-18](#)

## VPIM Messages

VPIM messages are made up of one or more MIME-encoded parts. The VPIM specification allows for optional MIME parts for spoken name and for forwarded and text messages. Cisco Unity Connection does not, however, support sending or receiving a vCard (an electronic business card that includes phone number, text name, and email address). If a vCard is attached to an outgoing or incoming message, Connection removes the vCard data. In addition, any attachments to messages other than the voice message and embedded messages are removed from outgoing and incoming messages.

Connection allows you to specify whether the recorded name of the sender is sent with outgoing messages. If incoming messages include a recorded name, it is played as part of the message. Connection can also be configured to update the directory with information from the header from incoming messages.

Figure 34-1 shows a sample VPIM message. Only a portion of the MIME encoding of the spoken name and voice message parts are shown because they are very long.

**Figure 34-1 Sample VPIM Message**

```

Date: Fri, 09 Feb 2007 17:39:03 GMT
From: Kelly Bader <4258001@connectiondomain1.cisco.com> ← From Address
To: 2534001@connectiondomain2.cisco.com ← To Address
MIME-Version: 1.0 (Voice 2.0)
Content-Type: Multipart/Voice-Message; Version=2.0
Boundary="MessageBoundary"
Content-Transfer-Encoding: 7bit
Message-ID:123456789
Subject: Testing
Sensitivity: Private
Importance: High

--MessageBoundary
Content-Type: Audio/32KADPCM ←
Content-Transfer-Encoding: Base64
Content-Disposition: inline; voice=Originator-Spoken-Name
Content-Language: en-US
Content-ID: part1@VM2-4321
 ← Spoken Name

glsfldslsertiflkTlpgkTpportrpkTpfgTpoiTpdadasssdadasdasd
<< The rest of the MIME encoding of the spoken name has been deleted. >>
fghgddfkgpokpeowrit09== ←

--MessageBoundary
Content-Type: Audio/32KADPCM ←
Content-Transfer-Encoding: Base64
Content-Description: VPIM Message
Content-Disposition: inline; voice=Voice-Message; filename=msg1.726
Content-Duration: 25
 ← Voice Message

u7wjOyRhws+krdns7Rju0t4tLF7cE0KoMxOTOnRWPn30c8uH9
<< The rest of the MIME encoding of the voice message has been deleted. >>
7/8e)Q== ←

```

191734

## VPIM Addresses

A VPIM address is in the same format as a typical SMTP email address: localpart@hostpart. The right-hand side of the address is the domain name of the system on the TCP/IP network that handles messages. The left-hand side of the address is a unique identifier for the user. Typically, the left-hand side is the user mailbox number or the mailbox number with a prefix.

For example, an outgoing VPIM message to Terry Campbell with the remote mailbox ID 2233 could be addressed:

To: 2233@remotevoicemailsysteem.com

If it is necessary to accommodate the numbering plan for your organization, the address can also contain a prefix:

To: 8882233@remotevoicemailsysteem.com

VPIM addresses are created by Cisco Unity Connection when sending VPIM messages; they are not entered by users when addressing messages.

## Message Addressing Options

### Revised May 2009

Cisco Unity Connection provides the following ways to address messages to individuals on a remote voice messaging system:

- **Connection directory**—When the List in Directory check box is checked for VPIM contacts, the Connection directory has the names and extensions for the VPIM contacts. Users can address messages to VPIM contacts the same way that they address messages to regular Connection users—by extension or by spelling the name of the recipient. Note that spoken name confirmation is available when a recorded name exists for the VPIM contact; if the contact does not have a recorded name, Connection uses Text to Speech to play the display name of the contact.
- **Blind addressing**—Blind addressing allows users to send messages to recipients at the VPIM location even if the recipients are not defined as contacts in the Connection directory. If the Allow Blind Addressing check box is checked on the VPIM Location page, users can address messages to recipients at this location by entering a number that is made up of the VPIM location Dial ID and the mailbox number of the recipient, or by saying the digits of the mailbox number and the display name of the VPIM location (for example, “five five at Seattle office”).
- **Distribution lists**—Users can address messages to a private or system distribution list that includes VPIM contacts so that the VPIM contact receives the message.

## Messaging Similarities and Limitations

For the most part, messaging between Cisco Unity Connection users and individuals on a remote voice messaging system is the same as messaging among Connection users. For example:

- Messages marked urgent when they are sent are marked urgent when they are retrieved by the recipient.
- Messages marked private when they are sent are marked private when they are retrieved by the recipient.
- Users can send messages to Connection distribution lists that include VPIM contacts.

Note the following exceptions:

- Requests for read receipts and delivery receipts are both returned as delivery receipts.
- In order for users on the remote voice messaging system to send messages to Connection distribution lists, the Accept Messages From Foreign System check box must be checked on the Edit Distribution List Basics page in Connection Administration. This check box is not checked by default.

## Audio Format Considerations

The Audio Format Conversion settings for the VPIM location (on the Networking > Edit VPIM Location page in Cisco Unity Connection Administration) allow you to control the audio format of outgoing and incoming VPIM messages, as follows:

- **Incoming Messages**—You can set whether incoming VPIM messages are stored in the format in which they were sent, or converted to the audio format that Cisco Unity Connection uses for recording messages.
- **Outbound Messages**—You can set whether outbound VPIM messages are sent in the format in which they were recorded, or converted to the G.726 codec.

To make decisions about these settings, consider the following:

- The audio format that the local Connection server uses for recording and playing voice messages.
- The audio format in which the remote voice messaging system can send and receive VPIM messages. Some voice messaging systems support only the G.726 format for VPIM messages, but you must consult the documentation of the remote voice messaging server to be sure.
- The network bandwidth.

We recommend that incoming VPIM messages be stored in the same audio format that the local Connection server uses for recording and playing messages.



## CHAPTER 35

# Creating Calendar Integrations

---

See the following sections:

- [About Calendar Integrations, page 35-1](#)
- [Creating a Calendar Integration with Exchange 2007, page 35-1](#)
- [Creating a Calendar Integration with Exchange 2003, page 35-10](#)
- [Creating a Calendar Integration with Cisco Unified MeetingPlace, page 35-18](#)
- [Creating a Calendar Integration with Cisco Unified MeetingPlace Express, page 35-25](#)

## About Calendar Integrations

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).

When integrated with Exchange 2007 or Exchange 2003, Connection also enables user to import Exchange contacts by using the Cisco Unity Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

## Creating a Calendar Integration with Exchange 2007

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.

## Task List for Creating a Calendar Integration with Exchange 2007

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 Integration](#)” section on page 35-2.
2. Configure Exchange 2007. See the “[Configuring Exchange 2007 for the Calendar Integration](#)” section on page 35-3.
3. Configure Connection. See the “[Configuring Cisco Unity Connection for the Exchange 2007 Calendar Integration](#)” section on page 35-5.
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 Connection users. See the “[Configuring Users for the Exchange 2007 Calendar Integration](#)” section on page 35-6.
6. Test the calendar integration. See the “[Testing the Exchange 2007 Calendar Integration](#)” section on page 35-7.
7. To teach users how to use the 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 7.x).
  - For importing Exchange contacts, see the “[Managing Your Personal Contacts](#)” chapter of the *User Guide for the Cisco Unity Connection Assistant Web Tool* (Release 7.x).
  - For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* (Release 7.x) at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/user/guide/pctr/7xcucugpctrx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/user/guide/pctr/7xcucugpctrx.html).

**Note**

You can change the Cisco Unity Connection configuration and the user configuration after the calendar integration is created. See the “[Changing the Cisco Unity Connection Configuration for the Exchange 2007 Calendar Integration](#)” section on page 35-8 and the “[Changing the User Configuration for the Exchange 2007 Calendar Integration](#)” section on page 35-8.

## Requirements for the Exchange 2007 Calendar Integration

**Revised May 2009**

The calendar integration with Exchange 2007 has the following requirements:

- Exchange 2007 as described in the “Requirements for Accessing Calendar Information for Meetings” section of *System Requirements for Cisco Unity Connection Release 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/requirements/7xcucsysreqs.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html).

- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/installation/guide/7xcucigx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html).

## Configuring Exchange 2007 for the Calendar Integration

Do the applicable procedure:

- If you are not using SSL for access to the Exchange 2007 server, do the “[To Configure Basic Access to Exchange 2007 for the Calendar Integration \(Without SSL\)](#)” procedure on page 35-3.
- 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 Integration \(With SSL\)](#)” procedure on page 35-4.

### To Configure Basic Access to Exchange 2007 for the Calendar Integration (Without SSL)

- 
- Step 1** On the Exchange server, open the **Exchange Management Console**.
- Step 2** Go to **Microsoft Exchange > Recipient Configuration > Mailbox**.
- Step 3** Right-click a mailbox that you want to enable for the calendar integration and click **Properties**.
- Step 4** In the Properties dialog box, click the **Mailbox Features** tab.
- Step 5** Click **Outlook Web Access** and click the **Enable** icon.
- Step 6** Click **OK**.
- Step 7** In the Exchange Management Console, go to **Microsoft Exchange > Server Configuration > Client Access**.
- Step 8** Click the **Outlook Web Access** tab in the lower-middle pane.
- Step 9** Right-click **OWA** and click **Properties**.
- Step 10** In the Properties dialog box, click the **Authentication** tab.
- Step 11** Click **Use One or More Standard Authentication Methods**.
- Step 12** Check the check boxes for one or more of the following options:
- Basic
  - Digest
  - Integrated Windows Authentication
- Step 13** Click **OK**.
- Step 14** 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 click **Properties**.
- Step 17** In the Properties dialog box, click the **Directory Security** tab.
- Step 18** Under Authentication and Access Control, click **Edit**.
- Step 19** Confirm that the enabled authentication schemes match those that you enabled in [Step 12](#).
- Step 20** Click **OK**.
- Step 21** In the Properties dialog box, click **OK**.

- Step 22** Open the **Exchange Management Shell**.
- Step 23** In the Exchange Management Shell, enter the following command:
- ```
iisbreset /noforce
```
- Step 24** Press **Enter**.

To Configure Secure Access to Exchange 2007 for the Calendar Integration (With SSL)



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 Integration”](#) section on page 35-5.

- 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 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 DNS name (recommended) so that the Connection server can successfully ping the Exchange server. Otherwise, the calendar 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 Connection to trust the Exchange 2007 server.

- Step 5** Enter the following command, where <path> is the location of the directory where the CA saves 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 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 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 “[Configuring Cisco Unity Connection for the Exchange 2007 Calendar Integration](#)” section on [page 35-5](#). 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 click **Properties**.
- Step 15** In the Properties dialog box, click the **Directory Security** tab.
- Step 16** Under Secure Communications, click **Edit**.
- Step 17** Check the **Require Secure Channel** check box.
- Step 18** Click **OK**.
- Step 19** In the Properties dialog box, click **OK**.
- 

## Configuring Cisco Unity Connection for the Exchange 2007 Calendar Integration

Do the following procedure.

### To Configure Cisco Unity Connection for the Exchange 2007 Calendar Integration

---

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** On the Search External Services page, click **Add New**.
- Step 3** On the New External Service page, in the Type list, click **Exchange 2007 External Service Template**.
- Step 4** Check the **Enabled** check box to enable the calendar 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, click the applicable setting to match the authentication mode that is used by the Exchange server.
- Step 8** In the Security Transport field, click the applicable setting:
- **None**—Connection does not use a secure connection with the Exchange 2007 server.
  - **SSL**—Connection uses an SSL connection with the Exchange 2007 server.
- Step 9** If you selected “SSL” and you want Connection to validate the Exchange 2007 server certificate, check the **Validate Server Certificate** check box.

**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 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** Click **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** Click **Save**.


## Configuring Users for the Exchange 2007 Calendar Integration



Do the following procedure.

**Note**

Exchange 2007 must have a user for each Connection user that you are configuring.

### To Configure Users for the Exchange 2007 Calendar Integration

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click 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 click **Search**.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**.
- Step 5** On the New External Service Accounts page, in the External Service field, click the display name that you entered in the [“To Configure Cisco Unity Connection for the Exchange 2007 Calendar Integration” procedure on page 35-5](#).
- Step 6** In the Email Address field, enter the email address in Exchange 2007 for the user.
- Step 7** In the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the Windows domain alias for the user is the same as the Connection user alias. Connection logs on the user with the Connection user alias.
  - **Use User ID Provided Below**—(*Recommended*) Enter the Windows domain alias for the user (useful when the User ID setting is different from the Connection user alias). Connection logs on 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 2007.
- Step 9** If known, in the Password field, enter the Windows domain password for the user. Connection logs on the user with the setting in this field.
-  **Note** If you leave the Password field blank, users must log on 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 Assistant Web Tool Release 7.x*.
- 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** Click **Save**.
- Step 12** To check the calendar configuration for the user, click **Test**. The Task Execution Results window appears with the test results.
- If any part of the test fails, verify the configuration for Exchange 2007, Cisco Unity Connection, and the user.
- Step 13** Repeat [Step 2](#) through [Step 12](#) for all remaining users.

## Testing the Exchange 2007 Calendar Integration

Do the following procedure.

### To Test the Configuration for the Exchange 2007 Calendar Integration

- Step 1** Log in to Outlook.
- Step 2** On the Go menu, click **Calendar**.
- Step 3** On the File menu, click **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** Click **Send**.
- Step 6** Log on 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.
- Connection reads the information about the Exchange 2007 meeting.

## Changing the Cisco Unity Connection Configuration for the Exchange 2007 Calendar Integration

You can change the Cisco Unity Connection configuration after the calendar integration was created. Do the following procedure.

### To Change the Cisco Unity Connection Configuration for the Exchange 2007 Calendar Integration

- 
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** On the Search External Services page, click the name of the external service that you created when you integrated Connection with Exchange 2007.
- Step 3** Check the **Enabled** check box to enable the external service.
- When this check box is not checked, the integration with Exchange 2007 is disabled.
- Step 4** In the Display Name field, enter a descriptive name.
- Step 5** In the Server field, enter the IP address or host name for the Exchange 2007 server.
- Step 6** In the Authentication Mode field, click the applicable setting to match the authentication mode that is used by the Exchange server.
- Step 7** In the Security Transport field, click the applicable setting:
- **None**—Connection does not use a secure connection with the Exchange 2007 server.
  - **SSL**—Connection uses an SSL connection with the Exchange 2007 server.
- Step 8** If you selected “SSL” and you want Connection to validate the Exchange 2007 server certificate, check the **Validate Server Certificate** check box.

**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 Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

- 
- Step 9** Under Service Capabilities, check the **User Access to Calendar and Personal Contacts** check box.
- Step 10** Click **Save**.
- Step 11** To check the integration with Exchange 2007, click **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange 2007 and Cisco Unity Connection.

---

## Changing the User Configuration for the Exchange 2007 Calendar Integration

You can change the user configuration after the calendar integration was created. Do the following procedure.

### To Change the User Configuration for the Exchange 2007 Calendar Integration

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

**Step 2** On the Search Users page, click 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 click **Search**.

**Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.

**Step 4** On the External Service Accounts page, in the Display Name column, click the display name for the Exchange 2007 service.

**Step 5** On the Edit External Services Account page, in the Email Address field, enter the email address in Exchange 2007 for the user.

**Step 6** In the Login Type field, click the applicable option:

- **Use Connection Alias**—This option is useful when the Windows domain alias for the user is the same as the Connection user alias. Connection logs on the user with the Connection user alias.
- **Use User ID Provided Below**—(*Recommended*) Enter the Windows domain alias for the user (useful when the User ID setting is different from the Connection user alias). Connection logs on the user with the setting in this field.

**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 Exchange 2007.

**Step 8** If known, in the Password field, enter the Windows domain password for the user. Connection logs on the user with the setting in this field.



**Note** If you leave the Password field blank, users must log on 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 Assistant Web Tool Release 7.x*.

**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** Click **Save**.

**Step 11** To check the calendar configuration for the user, click **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange 2007, Cisco Unity Connection, and the user.

# Creating a Calendar Integration with Exchange 2003

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 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.

## Task List for Creating a Calendar Integration with Exchange 2003

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 Integration”](#) section on page 35-10.
2. Configure Exchange 2003. See the [“Configuring Exchange 2003 for the Calendar Integration”](#) section on page 35-11.
3. Configure Connection. See the [“Configuring Cisco Unity Connection for the Exchange 2003 Calendar Integration”](#) section on page 35-14.
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 Connection users. See the [“Configuring Users for the Exchange 2003 Calendar Integration”](#) section on page 35-15.
6. Test the calendar integration. See the [“Testing the Exchange 2003 Calendar Integration”](#) section on page 35-16.
7. To teach users how to use the 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 7.x)*.
  - For importing Exchange contacts, see the [“Managing Your Personal Contacts”](#) chapter of the *User Guide for the Cisco Unity Connection Assistant Web Tool (Release 7.x)*.
  - For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool (Release 7.x)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/user/guide/pctr/7xcucugpctrx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/user/guide/pctr/7xcucugpctrx.html).

**Note**

You can change the Cisco Unity Connection configuration and the user configuration after the calendar integration is created. See the [“Changing the Cisco Unity Connection Configuration for the Exchange 2003 Calendar Integration”](#) section on page 35-16 and the [“Changing the User Configuration for the Exchange 2003 Calendar Integration”](#) section on page 35-17.

## Requirements for the Exchange 2003 Calendar Integration

Revised May 2009


The calendar integration with Exchange 2003 has the following requirements:

- Exchange 2003 as described in the “Requirements for Accessing Calendar Information for Meetings” section of *System Requirements for Cisco Unity Connection Release 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/requirements/7xcucsysreqs.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html).
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/installation/guide/7xcucigx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html).

## Configuring Exchange 2003 for the Calendar Integration

Do the applicable procedures.

### To Create the Privileged Service Account for the Exchange 2003 Calendar Integration

- 
- Step 1** On the Domain Controller, open **Active Directory Users and Computers**.
- Step 2** Right-click **Users** and click **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, go to **Microsoft Exchange > System Manager**.
- Step 5** Under Servers, right-click the server name and click **Properties**.
- Step 6** In the Properties dialog box, click the **Security** tab.
- Step 7** Click **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** Click **Check Names**.
- Step 9** Click **OK**.
- Step 10** In the list, click **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, click **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 Integration \(Without SSL\)](#)” procedure on page 35-11.

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 Integration \(With SSL\)](#)” procedure on page 35-13.

### To Configure Basic Access to Exchange 2003 for the Calendar Integration (Without SSL)

- 
- Step 1** On the Domain Controller, go to **Active Directory Users and Computers**.

- Step 2** Under Users, select all user accounts with calendars that you want Connection to access.
- Step 3** Right-click the highlighted users and click **Exchange Tasks**.
- Step 4** In the Exchange Tasks dialog box, click **Configure Exchange Features**.
- Step 5** Under Protocols, click **Outlook Web Access**.
- Step 6** Click the **Enable** icon.
- Step 7** Click **Next**.
- Step 8** Click **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** Click the **Settings** tab.
- Step 12** Confirm that the **Enable Forms Based Authentication** check box is unchecked.
- Step 13** Click **OK**.
- Step 14** Go to **Servers > <server name> > Protocols > HTTP > Exchange Virtual Server > Exchange**.
- Step 15** Right-click **Exchange** and click **Properties**.
- Step 16** In the Properties dialog box, click the **Access** tab.
- Step 17** Confirm that the following check boxes are checked:
- Read
  - Write
  - Directory Browsing
- Step 18** Click **Authentication**.
- Step 19** Confirm that one or more of the following options are enabled:
- Basic
  - Digest
  - Integrated Windows Authentication
- Step 20** Click **OK**.
- Step 21** In the Properties dialog box, click **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 click **Properties**.
- Step 25** In the Properties dialog box, click the **Directory Security** tab.
- Step 26** Under Authentication and Access Control, click **Edit**.
- Step 27** Confirm that the enabled authentication schemes match those that you enabled in [Step 19](#).
- Step 28** Click **OK**.
- Step 29** In the Properties dialog box, click **OK**.
-

**To Configure Secure Access to Exchange 2003 for the Calendar Integration (With SSL)**

**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 click **Properties**.

**Step 4** In the Properties dialog box, click the **Directory Security** tab.

**Step 5** Under Secure Communications, click **Server Certificate**.

**Step 6** Click **Next**.

**Step 7** Click **Create a New Certificate**.



**Note** If this option is not available, you must remove the existing certificate and do this step again.

**Step 8** Click **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 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 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 click **Properties**.

**Step 15** In the Properties dialog box, click the **Directory Security** tab.

**Step 16** Under Secure Communications, click **Server Certificate**.

**Step 17** Click **Next**.

**Step 18** Click **Process the Pending Request and Install the Certificate** and click **Next**.

**Step 19** Browse to the local file system and click the new certificate that CA sent.

**Step 20** Click **Next**.

**Step 21** Confirm that the certificate information is valid and click **Next**.

**Step 22** Click **Finish**.

**Step 23** In the Properties dialog box, click **OK**.

**Step 24** Return to the **IIS Manager** application.

**Step 25** Go to **IIS > <server name> > Web Sites > Default Web Site**.

**Step 26** Right-click **Default Web Site** and click **Properties**.

- Step 27** In the Properties dialog box, click the **Directory Security** tab.
- Step 28** Under Secure Communications, click **Edit**.
- Step 29** Check the **Require Secure Channel** check box.
- Step 30** Click **OK**.
- Step 31** In the Properties dialog box, click **OK**.
- 

## Configuring Cisco Unity Connection for the Exchange 2003 Calendar Integration

Do the following procedure.

### To Configure Cisco Unity Connection for the Exchange 2003 Calendar Integration

---

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** On the Search External Services page, click **Add New**.
- Step 3** On the New External Service page, in the Type list, click **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, click the applicable setting to match the authentication mode that is used by the Exchange server.
- Step 8** In the Security Transport field, click the applicable setting:
- **None**—Connection does not use a secure connection with the Exchange 2003 server.
  - **SSL**—Connection uses an SSL connection with the Exchange 2003 server.
- Step 9** If you selected “SSL” and you want Connection to validate the Exchange 2003 server certificate, check the **Validate Server Certificate** check box.



#### 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 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 alias for the privileged service account that Connection uses to log on to the Exchange 2003 server.
- 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 Connection uses to log on 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** Click **Save**.
- Step 14** To check the integration with Exchange 2003, click **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 Integration


Do the following procedure.



**Note**

Exchange 2003 must have a user for each Connection user that you are configuring.

### To Configure Users for the Exchange 2003 Calendar Integration

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click 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 click **Search**.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**.
- Step 5** On the New External Service Accounts page, in the External Service field, click the display name that you entered in the [“To Configure Cisco Unity Connection for the Exchange 2003 Calendar Integration” procedure on page 35-14](#).
- Step 6** In the Email Address field, enter the primary SMTP address in Exchange 2003 for the user.
- Step 7** In the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2003 is the same as the Connection user alias. Connection logs on the user with the 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 Connection user alias). Connection logs on 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 2003.
- 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** Click **Save**.
- Step 11** To check the calendar configuration for the user, click **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

Do the following procedure.

### To Test the Exchange 2003 Calendar Integration

- Step 1** Log in to Outlook.
- Step 2** On the Go menu, click **Calendar**.
- Step 3** On the File menu, click **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** Click **Send**.
- Step 6** Log on to the 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.
- Connection reads the information about the Exchange 2003 meeting.

## Changing the Cisco Unity Connection Configuration for the Exchange 2003 Calendar Integration

You can change the Cisco Unity Connection configuration after the calendar integration was created. Do the following procedure.

### To Change the Cisco Unity Connection Configuration for the Exchange 2003 Calendar Integration

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** On the Search External Services page, click the name of the external service that you created when you integrated Connection with Exchange 2003.

- Step 3** 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 4** In the Display Name field, enter a descriptive name.
- Step 5** In the Server field, enter the IP address or host name for the Exchange 2003 server.
- Step 6** In the Authentication Mode field, click the applicable setting to match the authentication mode that is used by the Exchange server.
- Step 7** In the Security Transport field, click the applicable setting:
- **None**—Connection does not use a secure connection with the Exchange 2003 server.
  - **SSL**—Connection uses an SSL connection with the Exchange 2003 server.
- Step 8** If you selected “SSL” and you want Connection to validate the Exchange 2003 server certificate, check the **Validate Server Certificate** check box.

**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 Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

- Step 9** In the Alias field, enter the Windows domain alias for the privileged service account that Connection uses to log on to the Exchange 2003 server.  
This setting must match the user ID for the privileged service account that is configured in Exchange 2003.
- Step 10** In the Password field, enter the password for the privileged service account that Connection uses to log on to the Exchange 2003 server.  
This setting must match the user password for the privileged service account that is configured in Exchange 2003.
- Step 11** Under Service Capabilities, check the **User Access to Calendar and Personal Contacts** check box.
- Step 12** Click **Save**.
- Step 13** To check the integration with Exchange 2003, click **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.

## Changing the User Configuration for the Exchange 2003 Calendar Integration

You can change the user configuration after the calendar integration was created. Do the following procedure.

### To Change the User Configuration for the Exchange 2003 Calendar Integration

- 
- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, in the Display Name column, click the display name for the Exchange 2003 service.
- Step 5** In the Email Address field, enter the primary SMTP address in Exchange 2003 for the user.
- Step 6** On the Edit External Services Account page, in the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2003 is the same as the Connection user alias. Connection logs on the user with the 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 Connection user alias). Connection logs on the user with the setting in this field.
- 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 Exchange 2003.
- Step 8** 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 9** Click **Save**.
- Step 10** To check the calendar configuration for the user, click **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.
- 

## Creating a Calendar Integration with Cisco Unified MeetingPlace

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.

### Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace

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”](#) section on page 35-19.
2. Configure Cisco Unified MeetingPlace. See the [“Configuring Cisco Unified MeetingPlace for the Calendar Integration”](#) section on page 35-19.

3. Configure Connection. See the “Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration” section on page 35-20.
4. Configure the Connection users. See the “Configuring Users for the Cisco Unified MeetingPlace Calendar Integration” section on page 35-21.
5. Test the calendar integration. See the “Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration” section on page 35-23.
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 7.x)*.

**Note**

You can change the Cisco Unity Connection configuration and the user configuration after the calendar integration is created. See the “Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Calendar Integration” section on page 35-23 and the “Changing the User Configuration for the Cisco Unified MeetingPlace Calendar Integration” section on page 35-24.

## Requirements for the Cisco Unified MeetingPlace Calendar Integration

### Revised May 2009

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 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/requirements/7xcucsysreqs.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html).
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/installation/guide/7xcucigx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html).

## Configuring Cisco Unified MeetingPlace for the Calendar Integration

Do the following procedure.

### To Configure Cisco Unified MeetingPlace for the Calendar Integration

- Step 1** Log on to the Cisco Unified MeetingPlace Administration Server as an administrator.
- Step 2** Click **User Configuration > User Profiles**.
- Step 3** Click **Add New**.
- Step 4** Enter the following values in the required fields to create a privileged service account:

|                      |                                                       |
|----------------------|-------------------------------------------------------|
| <b>First Name</b>    | Leave this field blank.                               |
| <b>Last Name</b>     | Enter <b>Cisco Unity Connection</b> .                 |
| <b>User ID</b>       | Enter <b>cucsyc</b> or another user ID that you want. |
| <b>User Password</b> | Enter the applicable password.                        |

|                         |                                        |
|-------------------------|----------------------------------------|
| <b>Profile Number</b>   | Enter the applicable profile number.   |
| <b>Profile Password</b> | Enter the applicable profile password. |
| <b>Type of User</b>     | Click <b>System Administrator</b> .    |

**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 35-20.

**Step 5** Click **Save**.

**Step 6** Log off of Cisco Unified MeetingPlace.

**Caution**

If you do not log off of Cisco Unified MeetingPlace, the test will fail in the [“To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration”](#) procedure on page 35-20.

### To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration

**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 log 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”](#) procedure on page 35-19.

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 click **External Services**.
- Step 2** On the Search External Services page, click **Add New**.
- Step 3** On the New External Service page, in the Type list, click **MeetingPlace 7.0 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 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, click the applicable setting:
- **None**—Connection does not use a secure connection with the Cisco Unified MeetingPlace server.
  - **SSL**—Connection uses an SSL connection with the Cisco Unified MeetingPlace server.
- Step 9** If you selected “SSL” and you want Connection to validate the Cisco Unified MeetingPlace server certificate, check the **Validate Server Certificate** check box.



**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 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 alias for the privileged service account that Connection uses to log on 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”](#) section on page 35-19.
- Step 11** In the Password field, enter the password for the privileged service account that Connection uses to log on 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”](#) section on page 35-19.
- 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** Click **Save**.
- Step 14** To check the integration with Cisco Unified MeetingPlace, click **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

Do the following procedure.

**Note**

Cisco Unified MeetingPlace must have an end user for each Connection user that you are configuring.

**To Configure Users for the Cisco Unified MeetingPlace Calendar Integration**

- 
- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**. The New External Service Account page appears.
- Step 5** In the External Service field, click the display name that you entered in the [“Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration”](#) section on page 35-20.
- Step 6** In the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the Cisco Unified MeetingPlace profile alias is the same as the Connection user alias. Connection logs on the user with the Connection user alias. Cisco Unified MeetingPlace provides information on public and private meetings to the user.
  - **Use Server Guest Account**—Connection logs on the user as a guest, without using the 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 Connection user alias). Connection logs on 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** Click **Save**.
- Step 10** To check the calendar configuration for the user, click **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

Do the following procedure.

### To Test the Configuration for the Cisco Unified MeetingPlace Calendar Integration

- 
- |               |                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Log in to Cisco Unified MeetingPlace as an end user.                                                                                                                                                           |
| <b>Step 2</b> | Click <b>Schedule</b> .                                                                                                                                                                                        |
| <b>Step 3</b> | 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.                                                            |
| <b>Step 4</b> | Log on to the Connection mailbox of the user that you invited to the Cisco Unified MeetingPlace meeting in <a href="#">Step 3</a> .                                                                            |
| <b>Step 5</b> | If the user account is configured for speech access, say <b>Play Meetings</b> .<br><br>If the user account is not configured for speech access, press <b>6</b> , and then follow the prompts to list meetings. |
| <b>Step 6</b> | When you hear the system announce the Cisco Unified MeetingPlace meeting that you just scheduled, either say <b>Join</b> , or press the applicable keys on the phone keypad to join the meeting.               |
- 

## Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Calendar Integration

You can change the Cisco Unity Connection configuration after the calendar integration was created. Do the following procedure.

### To Change the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Calendar Integration

- 
- |               |                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In Cisco Unity Connection Administration, expand <b>System Settings</b> , then click <b>External Services</b> .                                                                                                      |
| <b>Step 2</b> | On the Search External Services page, click the display name of the external service that you created when you integrated Connection with Cisco Unified MeetingPlace.                                                |
| <b>Step 3</b> | Verify that <b>MeetingPlace 7.0</b> is listed in the Display Name column for the integration.                                                                                                                        |
| <b>Step 4</b> | Click the display name of the external service that you created when you integrated Connection with Cisco Unified MeetingPlace.                                                                                      |
| <b>Step 5</b> | To enable the calendar integration, check the <b>Enabled</b> check box. To disable the calendar integration, uncheck the <b>Enabled</b> check box.                                                                   |
| <b>Step 6</b> | In the Display Name field, enter a descriptive name.                                                                                                                                                                 |
| <b>Step 7</b> | In the Server field, enter the IP address or host name for the Cisco Unified MeetingPlace server.                                                                                                                    |
| <b>Step 8</b> | In the Transfer Extension Dial String field, enter the digits that Connection must dial to transfer users on the phone to the opening greeting of Cisco Unified MeetingPlace server.                                 |
| <b>Step 9</b> | In the Security Transport field, click the applicable setting: <ul style="list-style-type: none"><li>• <b>None</b>—Connection does not use a secure connection with the Cisco Unified MeetingPlace server.</li></ul> |

- **SSL**—Connection uses an SSL connection with the Cisco Unified MeetingPlace server.

**Step 10** If you selected “SSL” and you want Connection to validate the Cisco Unified MeetingPlace server certificate, check the **Validate Server Certificate** check box.



**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 Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

**Step 11** In the Alias field, enter the Windows domain alias for the privileged service account that Connection uses to log on 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” section on page 35-19](#).

**Step 12** In the Password field, enter the password for the privileged service account that Connection uses to log on to the Cisco Unified MeetingPlace server.

This setting must match the User Password setting for the API user that you configured in the [“Configuring Cisco Unified MeetingPlace for the Calendar Integration” section on page 35-19](#).

**Step 13** 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.
- **MeetingPlace Scheduling and Joining**—Check this check box so that the user can schedule and join meetings.

**Step 14** Click **Save**.

**Step 15** To check the calendar configuration for the user, click **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.

## Changing the User Configuration for the Cisco Unified MeetingPlace Calendar Integration

You can change the user configuration after the calendar integration was created. Do the following procedure.

### To Change the User Configuration for the Cisco Unified MeetingPlace Calendar Integration

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

**Step 2** On the Search Users page, click the alias of a user.

**Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.

- Step 4** On the External Service Accounts page, in the Display Name column, click the display name for the Cisco Unified MeetingPlace service.
- Step 5** On the Edit External Service Account page, in the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the Cisco Unified MeetingPlace profile alias is the same as the Connection user alias. Connection logs on the user with the Connection user alias. Cisco Unified MeetingPlace provides information on public and private meetings to the user.
  - **Use Server Guest Account**—Connection logs on the user as a guest, without using the 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 Connection user alias). Connection logs on the user with the setting in this field. Cisco Unified MeetingPlace provides information on public and private meetings to the user.
- Step 6** *(Only when the Use User ID Provided Below option is selected in [Step 5](#))* In the User ID field, enter the User ID setting from Cisco Unified MeetingPlace.
- Step 7** 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 8** Click **Save**.
- Step 9** To check the calendar configuration for the user, click **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.
- 

## Creating a Calendar Integration with Cisco Unified MeetingPlace Express

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.

### Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace Express

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”](#) section on page 35-26.

2. Configure Cisco Unified MeetingPlace Express. See the “[Configuring Cisco Unified MeetingPlace Express for the Calendar Integration](#)” section on page 35-26.
3. Configure Connection. See the “[Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration](#)” section on page 35-27.
4. Configure the Connection users. See the “[Configuring Users for the Cisco Unified MeetingPlace Express Calendar Integration](#)” section on page 35-29.
5. Test the calendar integration. See the “[Testing the Cisco Unified MeetingPlace Express Calendar Integration](#)” section on page 35-30.
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 7.x)*.

**Note**

You can change the Cisco Unity Connection configuration and the user configuration after the calendar integration is created. See the “[Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Express Calendar Integration](#)” section on page 35-30 and the “[Changing the User Configuration for the Cisco Unified MeetingPlace Express Calendar Integration](#)” section on page 35-32.

## Requirements for the Cisco Unified MeetingPlace Express Calendar Integration

### Revised May 2009

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 7.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/7x/requirements/7xcucsysreqs.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html).
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection* at [http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html).

## Configuring Cisco Unified MeetingPlace Express for the Calendar Integration

Do the following procedure.

### To Configure Cisco Unified MeetingPlace Express for the Calendar Integration

- Step 1** Log on to Cisco Unified MeetingPlace Express and click **Administration**.
- Step 2** Click **User Configuration > User Profile Management**.
- Step 3** Click **Add New**.
- Step 4** Enter the following values in the required fields to create an API user:

|                   |                                                       |
|-------------------|-------------------------------------------------------|
| <b>First Name</b> | Leave this field blank.                               |
| <b>Last Name</b>  | Enter <b>Cisco Unity Connection</b> .                 |
| <b>User ID</b>    | Enter <b>cucsvc</b> or another user ID that you want. |

|                       |                                      |
|-----------------------|--------------------------------------|
| <b>User Password</b>  | Enter the applicable password.       |
| <b>Profile Number</b> | Enter the applicable profile number. |
| <b>Type of User</b>   | Click <b>API User</b> .              |



**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 35-27.

**Step 5** Click **Save**.

**Step 6** Log off of Cisco Unified MeetingPlace Express.



**Caution** If you do not log off of Cisco Unified MeetingPlace Express, the test will fail in the [“To Test the Cisco Unified MeetingPlace Express Configuration for the Calendar Integration”](#) procedure on page 35-27.

### To Test the Cisco Unified MeetingPlace Express Configuration for the Calendar Integration

**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 log 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”](#) procedure on page 35-26.

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 click **External Services**.

**Step 2** On the Search External Services page, click **Add New**.

**Step 3** On the New External Service page, in the Type list, click **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 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, click the applicable setting:
- **None**—Connection does not use a secure connection with the Cisco Unified MeetingPlace Express server.
  - **SSL**—Connection uses an SSL connection with the Cisco Unified MeetingPlace Express server.
- Step 9** If you selected “SSL” and you want Connection to validate the Cisco Unified MeetingPlace Express server certificate, check the **Validate Server Certificate** check box.

**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 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 alias for the API user that Connection uses to log on 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”](#) section on page 35-26.
- Step 11** In the Password field, enter the password for the API user that Connection uses to log on 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”](#) section on page 35-26.
- 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** Click **Save**.
- Step 14** To check the integration with Cisco Unified MeetingPlace Express, click **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

Do the following procedure.

**Note**

Cisco Unified MeetingPlace Express must have an end user for each Connection user that you are configuring.

### To Configure Users for the Cisco Unified MeetingPlace Express Calendar Integration

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**. The New External Service Accounts page appears.
- Step 5** In the External Service field, click the display name that you entered in the [“Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration”](#) section on page 35-27.
- Step 6** In the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the Cisco Unified MeetingPlace Express profile alias is the same as the Connection user alias. Connection logs on the user with the Connection user alias. Cisco Unified MeetingPlace Express provides information on public and private meetings to the user.
  - **Use Server Guest Account**—Connection logs on the user as a guest, without using the 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 Connection user alias). Connection logs on 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. Connection logs on 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** Click **Save**.

**Step 11** To check the calendar configuration for the user, click **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

Do the following procedure.

### To Test the Cisco Unified MeetingPlace Express Calendar Integration

---

**Step 1** Log in to Cisco Unified MeetingPlace Express as an end user.

**Step 2** Click **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** Log on to the 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.

---

## Changing the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Express Calendar Integration

You can change the Cisco Unity Connection configuration after the calendar integration was created. Do the following procedure.

### To Change the Cisco Unity Connection Configuration for the Cisco Unified MeetingPlace Express Calendar Integration

---

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.

**Step 2** On the Search External Services page, locate the external service that you created when you integrated Connection with Cisco Unified MeetingPlace Express.

- Step 3** Verify that **MeetingPlace Express 2.x** is listed in the Server Type column for the integration.
- Step 4** Click the name of the external service that you created when you integrated Connection with Cisco Unified MeetingPlace Express.
- Step 5** To enable the calendar integration, check the **Enabled** check box. To disable the calendar integration, uncheck the **Enabled** check box.
- Step 6** In the Display Name field, enter a descriptive name.
- Step 7** In the Server field, enter the IP address or the host name URL for the Cisco Unified MeetingPlace Express server.
- Step 8** In the Transfer Extension Dial String field, enter the digits that Connection must dial to transfer users on the phone to the opening greeting of Cisco Unified MeetingPlace Express server.
- Step 9** In the Security Transport field, click the applicable setting:
- **None**—Connection does not use a secure connection with the Cisco Unified MeetingPlace Express server.
  - **SSL**—Connection uses an SSL connection with the Cisco Unified MeetingPlace Express server.
- Step 10** If you selected “SSL” and you want Connection to validate the Cisco Unified MeetingPlace Express server certificate, check the **Validate Server Certificate** check box.

**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 Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

- Step 11** In the Alias field, enter the Windows domain alias for the API user that Connection uses to log on 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](#)” section on page 35-26.
- Step 12** In the Password field, enter the password for the API user that Connection uses to log on to the Cisco Unified MeetingPlace Express server.
- This setting must match the User Password setting for the API user that is configured in the “[Configuring Cisco Unified MeetingPlace Express for the Calendar Integration](#)” section on page 35-26.
- Step 13** Under Service Capabilities, check the applicable check boxes:
- **User Access to Calendar**—Check this check box so that the user hears their upcoming meetings.
  - **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 14** Click **Save**.
- Step 15** To check the calendar configuration for the user, click **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.

---

## Changing the User Configuration for the Cisco Unified MeetingPlace Express Calendar Integration

You can change the user configuration after the calendar integration was created. Do the following procedure.

### To Change the User Configuration for the Cisco Unified MeetingPlace Express Calendar Integration

---

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, in the Display Name column, click the display name for the Cisco Unified MeetingPlace Express service.
- Step 5** On the Edit External Service Account page, in the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the Cisco Unified MeetingPlace Express profile alias is the same as the Connection user alias. Connection logs on the user with the Connection user alias. Cisco Unified MeetingPlace Express provides information on public and private meetings to the user.
  - **Use Server Guest Account**—Connection logs on the user as a guest, without using the 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 Connection user alias). Connection logs on the user with the setting in this field. Cisco Unified MeetingPlace Express provides information on public and private meetings to the user.
- Step 6** *(Only when the Use User ID Provided Below option is selected in [Step 5](#))* In the User ID field, enter the User ID setting from Cisco Unified MeetingPlace Express.
- Step 7** *(Only if enabled)* In the User Profile Number field, enter the User ID setting from Cisco Unified MeetingPlace Express. Connection logs on the user with the setting in this field.
- Step 8** 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 9** Click **Save**.

**Step 10** To check the calendar configuration for the user, click **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.

---





# CHAPTER 36

## Configuring Service Parameters



### Caution

Information in this chapter is applicable in a standalone configuration only. If you have installed Cisco Unified Communications Manager Business Edition (CMBE), for information on configuring service parameters see the *Cisco Unified Communications Manager Administration Guide* at [http://www.cisco.com/en/US/products/ps7273/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html).

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 clicking the question mark button in the Service Parameter Configuration window. You can view the list with a particular parameter at the top by clicking that parameter.

If you deactivate a service in Cisco Unified Serviceability, Connection retains any updated service parameter values. If you start the service again, 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](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, page 36-1](#)
- [Description of Service Parameters, page 36-2](#)

## Configuring Service Parameters for a Cisco Unified Serviceability Service

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 click **Service Parameters**.
- Step 2** On the Service Parameters page, in the Server list, click the name of the Cisco Unity Connection server.
- Step 3** In the Service list, click 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, click **Set to Default**.

To view a list of parameters and their descriptions, click the ? button on the right side of the page.

- Step 5** Click **Save**.

## Description of Service Parameters

Revised May 2009

Table 36-1 describes the service parameters for Cisco Unity Connection.

**Table 36-1 Service Parameter Descriptions**

| Service Parameter            | Description                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cisco AMC Service</b>     |                                                                                                                                                                                                                                                                                     |
| 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><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><br>This is a required field.<br><br>Default setting: True                                                                                                    |
| Data Collection Polling Rate | Specifies the AMC collecting rate, in seconds.<br><br>This is a required field.<br><br>Default setting: 30<br>Minimum: 15<br>Maximum: 300<br>Unit: seconds                                                                                                                          |

**Table 36-1 Service Parameter Descriptions (continued)**

| Service Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Synchronization Period | <p>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.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the AMC service on the backup server for the parameter change to take effect.</p> <p>Default setting: 60<br/>Minimum: 15<br/>Maximum: 300<br/>Unit: seconds</p> |
| RMI Registry Port Number      | <p>Specifies the port number to activate 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.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the AMC service for the parameter change to take effect.</p> <p>Default setting: 1099<br/>Minimum: 1024<br/>Maximum: 65535</p>                                                                                                                |
| RMI Object Port Number        | <p>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.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the AMC service for the parameter change to take effect.</p> <p>Default setting: 1090<br/>Minimum: 1024<br/>Maximum: 65535</p>                                                                                                                                            |
| AlertMgr Enabled              | <p><i>(For AMC troubleshooting purpose only.)</i> Enables and disables the alerting (email/epage) feature.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the AMC service for the parameter change to take effect.</p> <p>Default setting: True</p>                                                                                                                                                                                                                       |

**Table 36-1 Service Parameter Descriptions (continued)**

| Service Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logger Enabled                              | <p>(For AMC troubleshooting purpose only.) Enables and disables the logging feature (CSV files for generating reports).</p> <p>This is a required field.</p> <p><b>Note</b> Restart the AMC service for the parameter change to take effect.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Cisco Database Layer Monitor Service</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Maintenance Time                            | <p>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.</p> <p>This is a required field.</p> <p>Default setting: 24<br/>Minimum: 1<br/>Maximum: 24<br/>Unit: hours</p>                                                                        |
| Maintenance Window                          | <p>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.</p> <p>This is a required field.</p> <p>Default setting: 2<br/>Minimum: 1<br/>Maximum: 24<br/>Unit: hours</p> |

**Table 36-1**      **Service Parameter Descriptions (continued)**

| Service Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MaintenanceTaskTrace                   | <p>Sets the Maintenance Task trace. You must turn on this parameter to get a performance counter trace from the Maintenance Task.</p> <p>This is a required field.</p> <p>Default setting: Off</p>                                                                                                                                                               |
| <b>Cisco DirSync</b>                   |                                                                                                                                                                                                                                                                                                                                                                  |
| Maximum Number of Agreements           | <p>Specifies maximum numbers of agreements that can be configured from the Plugin GUI.</p> <p>This is a required field.</p> <p><b>Note</b>    Restart Plugin GUI.</p> <p>Default setting: 3<br/>Minimum: 1<br/>Maximum: 5</p>                                                                                                                                    |
| Maximum Number of Hosts                | <p>Specifies the maximum number of hosts that can be configured for failover purpose.</p> <p>This is a required field.</p> <p><b>Note</b>    Restart Plugin GUI.</p> <p>Default setting: 3<br/>Minimum: 1<br/>Maximum: 3</p>                                                                                                                                     |
| Retry Delay on Host Failure (secs)     | <p>Specifies the delay used in retry logic in case of LDAP connection failure.</p> <p>This is a required field.</p> <p><b>Note</b>    Parameter change takes effect automatically.</p> <p>Default setting: 5<br/>Minimum: 5<br/>Maximum: 60</p>                                                                                                                  |
| Retry Delay on HostList Failure (mins) | <p>Specifies the delay used in retry logic in case of LDAP connection failure. Unlike Retry Delay on Host Failure, the delay is applied when retry starts over again on the whole host list.</p> <p>This is a required field.</p> <p><b>Note</b>    Parameter change takes effect automatically.</p> <p>Default setting: 10<br/>Minimum: 10<br/>Maximum: 120</p> |

**Table 36-1**      **Service Parameter Descriptions (continued)**

| Service Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP Connection Timeout (secs)             | <p>Specifies the timeout period (in seconds) used for establishing the LDAP connection. The LDAP service provider aborts the connection attempt if a connection cannot be established in the specified timeout period.</p> <p>This is a required field.</p> <p><b>Note</b>    Parameter change takes effect automatically.</p> <p>Default setting: 5<br/>Minimum: 1<br/>Maximum: 60</p> |
| Delayed Sync Start Time (mins)             | <p>Specifies the delay applied before starting a synchronization process when the Cisco DirSync application starts.</p> <p>This is a required field.</p> <p><b>Note</b>    Restart the Cisco Tomcat service for the parameter change to take effect.</p> <p>Default setting: 5<br/>Minimum: 5<br/>Maximum: 60</p>                                                                       |
| <b>Cisco RIS Data Collector Parameters</b> |                                                                                                                                                                                                                                                                                                                                                                                         |
| RIS Cluster TCP Port                       | <p>Specifies the static TCP port that the Cisco RIS Data Collector services use to communicate with each other.</p> <p>This is a required field.</p> <p><b>Note</b>    Restart the Cisco RIS Data Collector service for the parameter change to take effect.</p> <p>Default setting: 2555<br/>Minimum: 1024<br/>Maximum: 65535</p>                                                      |
| RIS Client TCP Port                        | <p>Specifies the static TCP port that the RIS clients use to communicate with the Cisco RIS Data Collector services.</p> <p>This is a required field.</p> <p><b>Note</b>    Restart Cisco Database Layer Monitor service and the Cisco RIS Data Collector services for the parameter change to take effect.</p> <p>Default setting: 2556<br/>Minimum: 1024<br/>Maximum: 65535</p>       |

**Table 36-1**      **Service Parameter Descriptions (continued)**

| <b>Service Parameter</b>                         | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RIS Client Timeout                               | <p>Specifies the time, in seconds, that a RIS client waits for a reply from the Cisco RIS Data Collector service.</p> <p>This is a required field.</p> <p>Default setting: 15<br/>Minimum: 10<br/>Maximum: 1000<br/>Unit: seconds</p>                                                                                                                                                                                                                 |
| RIS Cleanup Time of the Day                      | <p>Specifies the time of the day that the RIS database is cleaned up to remove any unused or old device information. During this time, the NumofRegistrationAttempts performance counters for all devices reset to 0.</p> <p>This is a required field.</p> <p>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</p>                                          |
| RIS Unused Cisco CallManager Device Store Period | <p>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, the expired entries are removed during the next RIS database cleanup time (specified in the RIS Cleanup Time of the Day parameter).</p> <p>This is a required field.</p> <p>Default setting: 3<br/>Minimum: 1<br/>Maximum: 30<br/>Unit: days</p> |
| RIS Unused CTI Records Storage Period            | <p>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).</p> <p>This is a required field.</p> <p>Default setting: 1<br/>Minimum: 0<br/>Maximum: 5<br/>Unit: days</p> |

**Table 36-1**      **Service Parameter Descriptions (continued)**

| Service Parameter                        | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RIS Maximum Number of Unused CTI Records | <p>Specifies the maximum number of records for closed CTI providers, devices, and lines that are kept in the RIS database. After the limit specified in this parameter is reached, Cisco CTI Manager does not save any new records for unused CTI providers, devices, or lines to the RIS database.</p> <p>This is a required field.</p> <p>Default setting: 3000<br/>Minimum: 0<br/>Maximum: 5000<br/>Unit: records</p> |
| TLC Throttling Enabled                   | <p>Enables or disables Trace and Log Central throttling behavior.</p> <p>This is a required field.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                                                      |
| TLC Throttling IOWait Goal               | <p>Specifies the system IOWait percentage that TLC throttles itself toward.</p> <p>This is a required field.</p> <p>Default setting: 10<br/>Minimum: 10<br/>Maximum: 40</p>                                                                                                                                                                                                                                              |
| TLC Throttling CPU Goal                  | <p>Specifies the system CPU utilization percentage that TLC throttles itself toward.</p> <p>This is a required field.</p> <p>Default setting: 80<br/>Minimum: 65<br/>Maximum: 90</p>                                                                                                                                                                                                                                     |
| TLC Throttling Polling Delay             | <p>Specifies the minimum delay in milliseconds between IO wait and CPU usage polls for the purpose of trace collection throttling.</p> <p>This is a required field.</p> <p>Default setting: 250<br/>Minimum: 200<br/>Maximum: 2000</p>                                                                                                                                                                                   |
| TLC Throttling SFTP Maximum Delay        | <p>Specifies the maximum time an SFTP transfer is paused in order to prevent timeouts.</p> <p>This is a required field.</p> <p>Default setting: 5000<br/>Minimum: 1000<br/>Maximum: 10000</p>                                                                                                                                                                                                                            |

**Table 36-1 Service Parameter Descriptions (continued)**

| Service Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Number of Processes and Threads | <p>Specifies the maximum number of Processes and Threads allowed for SystemAccess to provide the complete Process and Thread statistics counters. If the total number of Processes/Threads has exceeded this maximum number, SystemAccess only provides up to the maximum number of Processes statistics counters, and none of the other Thread statistics counters are provided.</p> <p>This is a required field.</p> <p>Default setting: 2000<br/>Minimum: 1000<br/>Maximum: 3000</p>                                                                       |
| Enable Logging                          | <p>Determines whether collecting and logging of troubleshooting perfmon data is enabled (True) or disabled (False).</p> <p>This is a required field.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                                                                                                                                         |
| Polling Rate                            | <p>Specifies the troubleshooting perfmon data polling rate, in seconds.</p> <p>This is a required field.</p> <p>Default setting: 15<br/>Minimum: 5<br/>Maximum: 300<br/>Unit: seconds</p>                                                                                                                                                                                                                                                                                                                                                                     |
| Maximum No. of Files                    | <p>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, we recommend that the Maximum File Size be reduced.</p> <p>This is a required field.</p> <p><b>Note</b> If this value is reduced, excessive log files with the oldest timestamp are deleted if Troubleshooting Perfmon Data Logging is enabled and RISDC is activated. You can save these files first before changing Maximum No. of Files.</p> <p>Default setting: 50<br/>Minimum: 1<br/>Maximum: 100</p> |
| Maximum File Size (MB)                  | <p>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, we recommend that the Maximum No. of Files be reduced.</p> <p>This is a required field.</p> <p>Default setting: 5<br/>Minimum: 1<br/>Maximum: 500</p>                                                                                                                                                                                                                          |

Cisco Serviceability Reporter

**Table 36-1**      **Service Parameter Descriptions (continued)**

| Service Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RTMT Reporter Designated Node | <p>Specifies the designated node on which RTMTReporter runs. Note that the RTMTReporter service is CPU-intensive. This field is automatically filled in with the local node IP at which Reporter is first activated.</p> <p>This is a required field.</p>                                                                                                                       |
| RTMT Report Generation Time   | <p>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.</p> <p>This is a required field.</p> <p>Default setting: 30<br/>Minimum: 0<br/>Maximum: 1200</p>                                                  |
| RTMT Report Deletion Age      | <p>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 are deleted on the eighth day. A value of 0 disables report generation, and any existing reports are deleted.</p> <p>This is a required field.</p> <p>Default setting: 7<br/>Minimum: 0<br/>Maximum: 30</p> |



## CHAPTER 37

# Configuring Enterprise Parameters

---



### Caution

Information in this chapter is applicable in a standalone configuration only. If you have installed Cisco Unified Communications Manager Business Edition (CMBE), for information on configuring enterprise parameters, see the *Cisco Unified Communications Manager Administration Guide* at [http://www.cisco.com/en/US/products/ps7273/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html).

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, page 37-1](#)
- [Description of Enterprise Parameters, page 37-2](#)

## Configuring Enterprise Parameters for Cisco Unified Serviceability Services

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 click **Enterprise Parameters**.
- Step 2** On the Enterprise Parameters Configuration page, enter the applicable settings. To set all service parameters to the default values, click **Set to Default**.

To view a list of enterprise parameters and their descriptions, click the ? button on the right side of the page.

**Step 3** Click **Save**.

---

## Description of Enterprise Parameters

**Revised May 2009**

Table 37-1 describes the enterprise parameters available in Cisco Unity Connection. Note that only the following enterprise parameters apply to Cisco Unity Connection:

- [Max Number of Device Level Trace](#)
- [Trace Compression](#)
- [Default Network Locale](#)
- [Default User Locale](#)
- [File Close Thread Flag](#)
- [FileCloseThreadQueueWaterMark](#)
- [Service Manager TCP Server Communication Port Number](#)
- [Service Manager TCP Client Communication Port Number](#)
- [Organization Top Level Domain](#)
- [Cluster Fully Qualified Domain Name](#)
- [Cisco Support Use 1](#)
- [Remote Syslog Server Name](#)
- [Syslog Severity for Remote Syslog Messages](#)
- [Report Socket Connection Timeout](#)
- [Report Socket Read Timeout](#)

**Table 37-1 Enterprise Parameter Descriptions**

| Enterprise Parameter                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Synchronization Between Auto Device Profile and Phone Configuration | <p>(Cisco Unified Communications Manager only) Determines whether the auto device profile in Cisco Unified CM Administration (Device &gt; Device Settings) is updated when an update occurs to the phone configuration, including directory numbers, speed dials, and subscribed IP phone services. Valid values specify True (Cisco Unified CM updates the auto device profile when it updates the phone configuration) or False (Cisco Unified CM does not update the auto device profile when it updates phone configuration).</p> <p>This is a required field.</p> <p>Default setting: True</p> |
| Max Number of Device Level Trace                                    | <p>Specifies how many devices can be traced concurrently if device name-based trace is selected in Trace Configuration in Cisco Unified Serviceability.</p> <p>This is a required field.</p> <p>Default setting: 12<br/>Minimum: 0<br/>Maximum: 256</p>                                                                                                                                                                                                                                                                                                                                             |
| Trace Compression                                                   | <p>Determines whether or not to compress trace files as they are being written.</p> <p>This is a required field.</p> <p>Default setting: Disabled</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DSCP for Phone-based Services                                       | <p>(Cisco Unified Communications Manager only) Specifies the Differentiated Service Code Point (DSCP) IP classification for IP phone services on phones, including any HTTP traffic.</p> <p>This is a required field.</p> <p><b>Note</b> Restart phones for the parameter change to take effect.</p> <p>Default setting: default DSCP (000000)</p>                                                                                                                                                                                                                                                  |
| DSCP for Phone Configuration                                        | <p>(Cisco Unified Communications Manager only) Specifies the Differentiated Service Code Point (DSCP) IP classification for any phone configuration, including any TFTP, DNS, or DHCP access that is necessary for phone configuration.</p> <p>This is a required field.</p> <p><b>Note</b> Restart phones for the parameter change to take effect.</p> <p>Default setting: CS3 (precedence 3) DSCP (011000)</p>                                                                                                                                                                                    |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSCP for Cisco CallManager to Device Interface | <p>(Cisco Unified Communications Manager only) Specifies the Differentiated Service Code Point (DSCP) IP classification for protocol control interfaces that are used in Cisco Unified CM-to-device communications.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the Cisco CallManager service and associated devices for the parameter change to take effect.</p> <p>Default setting: CS3 (precedence 3) DSCP (011000)</p> |
| Connection Monitor Duration                    | <p>(Cisco Unified Communications Manager only) Specifies the a common link qualifying time period for all the devices using a specific SRST reference.</p> <p>This is a required field.</p> <p><b>Note</b> Restart all services for the parameter change to take effect.</p> <p>Default setting: 120<br/>Minimum: 0<br/>Maximum: 2592000</p>                                                                                               |
| Auto Registration Phone Protocol               | <p>(Cisco Unified Communications Manager only) Specifies the protocol that auto-registered phones should boot with during initialization.</p> <p>This is a required field.</p> <p><b>Note</b> Restart all services for the parameter change to take effect.</p> <p>Default setting: SCCP</p>                                                                                                                                               |
| BLF for Call Lists                             | <p>(Cisco Unified Communications Manager only) Specifies the default Busy Lamp Field (BLF) behavior for phones.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the phones for the parameter change to take effect.</p> <p>Default setting: Disabled</p>                                                                                                                                                                       |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advertise G.722 Codec      | <p>(Cisco Unified Communications Manager only) Determines whether Cisco Unified IP Phones advertise the G.722 codec to Cisco Unified CM. Codec negotiation involves two steps: first, the phone must advertise the supported codecs to Cisco Unified CM (not all phone models support the same set of codecs). Second, when Cisco Unified CM receives the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. This parameter only applies to Cisco Unified IP Phone models 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE. Valid values specify True (the specified Cisco Unified IP Phone models advertise G.722 to Cisco Unified CM) or False (the specified Cisco Unified IP Phone models do not advertise G.722 to Cisco Unified CM).</p> <p>This is a required field.</p> <p><b>Note</b> Restart the phones for the parameter change to take effect.</p> <p>Default setting: Enabled</p> |
| Phone Personalization      | <p>(Cisco Unified Communications Manager only) Specifies the default value for Phone Personalization.</p> <p>This is a required field.</p> <p>Default setting: 0</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Services Provisioning      | <p>(Cisco Unified Communications Manager only) A new device configuration parameter is added to control whether the phone uses the services provisioned in the configuration file (Internal) or the services received from the URLs (External URLs) or both. This parameter is required for backward-compatibility with third-party provisioning servers, mainly the ability to disable the new provisioning mechanism so that the phone presents only those services coming from the Services URL.</p> <p>This is a required field.</p> <p>Default setting: Internal</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CCMAdmin Parameters</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max List Box Items        | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of items that display in a list box in Cisco Unified CM Administration; for any value above the number that is specified in this parameter, only the default (such as None) and the currently selected items appear in the list box, and a lookup button appears to the right of the list box. Click the lookup button to find and choose the desired item. Increasing the value above the default sends more items directly to the browser but results in slower page loads in a large system. Decreasing the value sends fewer items directly to the browser and results in faster page load for a large system. This setting affects only fields where a large number of user-defined items are likely, such as Partition, Calling Search Space, and Voice Mail Profile. This is a required field.</p> <p><b>Note</b> Click Save, close the browser, and open a new one for the change to take effect.</p> <p>Default setting: 250<br/>Minimum: 50<br/>Maximum: 9999</p> |
| Max Lookup Items          | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of items that are sent to the browser when doing a lookup. Using a higher value sends more items directly to the lookup browser window (results in slower page load but faster searching). Using a lower value sends fewer items directly to the lookup browser window (results in faster page load but slower search). This is a required field.</p> <p><b>Note</b> Click Save, close the browser, and open a new one for the change to take effect.</p> <p>Default setting: 1000<br/>Minimum: 250<br/>Maximum: 9999</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Enable Dependency Records | <p>(Cisco Unified Communications Manager only) Determines whether to display dependency records. Valid values specify True (display dependency records) or False (do not display dependency records). This is a required field.</p> <p><b>Note</b> Displaying dependency records leads to high CPU usage and may affect call processing. It may take a long time to execute. If you monitor CPU usage, you might see high CPU usage alarms. To avoid possible performance issues, display dependency records only during off-peak hours or during the next maintenance window.</p> <p>Default setting: False</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Select DN on Any Partition | <p>(Cisco Unified Communications Manager only) Specifies whether the directory number configuration page automatically selects the first matching DN to populate the page. The default is False, which means the DN/Partition name is used to populate the DN page. If the parameter is set to True and the DN is changed, the first entry matching the DN is used to populate the page.</p> <p>This is a required field.</p> <p><b>Note</b> Click the Save button.</p> <p>Default setting: False</p>                                                                             |
| <b>CCMUser Parameters</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Show Ring Settings              | <p>(Cisco Unified Communications Manager only) Determines whether the option to change the Ring Settings on a phone appears on the Cisco CallManager User Options (CCMUser) window. Valid values specify True (enabled) or False (disabled). If this parameter is enabled and the current device of the user supports the Ring Setting feature, the user can view and change the Ring Settings for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: False</p> |
| Show Call Forwarding            | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Call Forwarding on a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the Call Forwarding feature, the user can view and change the Call Forward Settings for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: Show All Settings</p>                                                                      |
| Show Speed Dial Settings        | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Add/Update Speed Dial Settings on a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the Speed Dialing feature, the user can view and change the Speed Dial Settings for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                        |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show Cisco IP Phone Services Settings     | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether or not the option IP Phone Services on a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the IP Phone Services feature, the user can view and change the IP Phone Services Settings for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                 |
| Show Personal Address Book Settings       | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether or not the option Personal Address Book on a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the Personal Address Book feature, the user can view and change the Personal Address Book Settings for that device.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>This is a required field.</p> <p>Default setting: True</p>                     |
| Show Message Waiting Lamp Policy Settings | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether or not the option Message Waiting Lamp Policy on a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the Message Waiting Lamp Policy feature, the user can view and change the Message Waiting Lamp Policy Settings for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>   |
| Show Line Text Label Settings             | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether or not the option to configure Line Text Label for a phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user has lines configured, the user can view and change the Line Text Label for each line on that phone unless the line is the Primary Line.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: False</p> |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show Locale for Phone Settings     | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Change Locale for this Phone appears on the Cisco CallManager User Options (CCMUser) window. If the current device of the user supports the Localization feature, the user can view and change the User Locale Setting for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p> |
| Show Locale for Web Pages Settings | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Locale for Web Pages appears on the Cisco CallManager User Options (CCMUser) window. If this option is enabled, the user can view and change the User Locale Setting Extension Mobility and CCMUser Web Pages.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                          |
| Show Change Password Option        | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Change Password for a User appears on the Cisco CallManager User Options (CCMUser) window. If this option is enabled, the user can change the Password.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                 |
| Show Change PIN Option             | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Change PIN for a User appears on the Cisco CallManager User Options (CCMUser) window. If this option is enabled, the user can change the PIN.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                           |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show Download Plugin Option    | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Download/Install Plugins for a User appears on the Cisco CallManager User Options (CCMUser) window. If this option is enabled, the user can Download/Install Plugins.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                                                 |
| Show Online Guide Option       | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Online Phone Guide appears on the Cisco IP Phone Options web (CCMUser). If the current device of the user supports the Online Phone Guide feature, the user can view the Online Guide for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                |
| Show Directory                 | <p>(Cisco Unified Communications Manager only) Determines whether or not the option Directory appears on the Cisco IP Phone Options web (CCMUser). If this option is enabled, the user can search directory.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                                                                                              |
| Show Mobility Features Option  | <p>(Cisco Unified Communications Manager only) Determines whether or not the option to access Remote Destinations and Access Lists appears on the Cisco IP Phone Options web (CCMUser). If the current device of the user supports the Remote Destinations and Access Lists feature, the user can view the configure Remote Destination and Access Lists for that device.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p> |
| Show Manager Name in Directory | <p>(Cisco Unified Communications Manager only) Determines whether or not to display the Manager Name in the Directory Find List.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                          |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show User ID in Directory      | <p>(Cisco Unified Communications Manager only) Determines whether or not to display the Manager Name in the Directory Find List.</p> <p>This is a required field.</p> <p><b>Note</b> Change takes effect on next login to Cisco CallManager User Options window.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CDR Parameters</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CDR File Time Interval         | <p>(Cisco Unified Communications Manager only) Specifies the time interval for collecting CDR data. For example, if this value is set to 1, each file contains 1 minute of CDR data (CDRs and CMRs, if enabled). The CDR database does not receive the data in each file until the interval has expired, so consider how quickly you want access to the CDR data when you decide what interval to set in this parameter. For example, setting this parameter to 60 means that each file contains 60 minutes worth of data, but that data is not available until the 60-minute period has elapsed and the records are written to the CDR database.</p> <p>This is a required field.</p> <p>Default setting: 1<br/>Minimum: 0<br/>Maximum: 1440<br/>Unit: min</p> |
| Cluster ID                     | <p>(Cisco Unified Communications Manager only) Provides a unique identifier for this cluster. Because this parameter is used in CDRs, collections of CDRs from multiple clusters can be traced to the sources.</p> <p>This is a required field.</p> <p>Default setting: StandAloneCluster<br/>Maximum length: 50<br/>Allowed values: Provide a valid cluster ID that uses the characters A-Z, a-z, 0-9, ., -</p>                                                                                                                                                                                                                                                                                                                                                |
| <b>Localization Parameters</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Default Network Locale         | <p>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.</p> <p>This is a required field.</p> <p><b>Note</b> 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.</p> <p>Default setting: United States</p>                                                                                                                                                                                                                                                 |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default User Locale     | <p>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.</p> <p>This is a required field.</p> <p><b>Note</b> Reset all devices for the parameter change to take effect.</p> <p>Default setting: English United States</p>                                                                                                                                                                                                                                                                                                                                     |
| <b>MLPP Parameters</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| MLPP Domain Identifier  | <p><i>(Cisco Unified Communications Manager only)</i> Specifies the service domain used by Multi-Level Precedence and Preemption (MLPP). The MLPP service applies to an MLPP domain only. Connections and resources that belong to a call from an MLPP user get marked with a Precedence level and MLPP domain identifier that only calls of higher Precedence from MLPP users in the same MLPP domain can preempt. This parameter accepts hexadecimal values (values starting with 0x). You can reset all devices by resetting every device pool in the system.</p> <p>This is a required field.</p> <p><b>Note</b> Reset all devices for the parameter change to take effect.</p> <p>Default setting: 000000</p> |
| MLPP Indication Status  | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether the device should apply Multi-Level Precedence and Preemption (MLPP) services such as tones, special displays and sending of MLPP/precedence-related Precedence information element (IE) and values in Signal and Cause IEs.</p> <p>This is a required field.</p> <p><b>Note</b> Reset all devices for the parameter change to take effect.</p> <p>Default setting: MLPP Indication turned off.</p>                                                                                                                                                                                                                                       |
| MLPP Preemption Setting | <p><i>(Cisco Unified Communications Manager only)</i> Determines whether a device should apply preemption and preemption signaling (preemption tones/information elements) to accommodate higher precedence calls. Valid values specify No Preemption Allowed and Forceful Preemption (lower precedence calls terminate when a higher precedence call arrives that, to complete the call, needs the resource that the lower precedence call currently uses). You can reset all devices by resetting every device pool in the system.</p> <p>This is a required field.</p> <p><b>Note</b> Reset all devices for the parameter change to take effect.</p> <p>Default setting: No preemption allowed.</p>             |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Precedence Alternate Party Timeout            | <p>(Cisco Unified Communications Manager only) Specifies the maximum time to wait before diverting a call to the predetermined alternate party when the called party has MLPP Alternate Party Settings specified in the Directory Number Configuration and the called party does not acknowledge preemption or does not answer a precedence call before this timer expires.</p> <p>This is a required field.</p> <p>Default setting: 30<br/>Minimum: 4<br/>Maximum: 60<br/>Unit: sec</p>                                                                                                                                                                  |
| Use Standard VM Handling for Precedence Calls | <p>(Cisco Unified Communications Manager only) Determines whether a precedence call is forwarded to the voice-messaging system, such as when no answer or busy signal occurs. If this parameter is set to False, precedence calls do not get forwarded to the voice-messaging system. If this parameter is set to True, precedence calls forward to the voice-messaging system. For Multi-Level Precedence and Preemption (MLPP), we recommend that a voice-messaging system does not answer precedence calls; rather, configure the system so that MLPP calls forward to an operator.</p> <p>This is a required field.</p> <p>Default setting: False</p> |
| <b>Security Parameters</b>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Cluster Security Mode                         | <p>(Cisco Unified Communications Manager only) Indicates the security mode of the cluster. A value of 0 indicates Non Secure (phones register in non-secure mode [no security]); 1 indicates Mixed (the cluster allows the registration of both secure devices and non-secure devices). Because this parameter is read-only, to change the cluster security mode, you must run the CTL Client plugin.</p> <p>This is a required field.</p> <p><b>Note</b> Restart Cisco CallManager service for the parameter change to take effect.</p> <p>Default setting: 0</p>                                                                                        |
| CAPF Phone Port                               | <p>(Cisco Unified Communications Manager only) Specifies the port that the Cisco Authority Proxy Function Service listens to requests from a phone for a Certificate.</p> <p>This is a required field.</p> <p><b>Note</b> Restart the Cisco CAPF Service for this parameter change to take effect.</p> <p>Default setting: 3804<br/>Minimum: 1023<br/>Maximum: 55556</p>                                                                                                                                                                                                                                                                                  |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CAPF Operation Expires in (Days) | <p>(Cisco Unified Communications Manager only) Specifies the number of days in which any CAPF operation must be completed. This parameter affects all phones that use CAPF.</p> <p>This is a required field.</p> <p>Default setting: 10<br/>Minimum: 1<br/>Maximum: 365</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Enable Caching                   | <p>(Cisco Unified Communications Manager only) Causes credentials to be stored in memory for up to 2 minutes. This could save time if a credential is used often, by using memory, rather than making a query of the database to authenticate.</p> <p>This is a required field.</p> <p>Default setting: False</p>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Phone URL Parameters</b>      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| URL Authentication               | <p>(Cisco Unified Communications Manager only) Specifies the URL that points to a web page that resides in one of the Cisco CallManager Cisco IP Phone (CCMCIP) webs in the cluster. This URL provides an authentication proxy service between Cisco IP Phone models 7940/7945/7960/7965/7970 and the LDAP directory. This URL is used to validate requests made directly to the phone. This URL is automatically configured at install time. If the URL is removed, the push capabilities to the Cisco IP Phones are disabled.</p> <p>Maximum length: 255<br/>Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p> |
| URL Directories                  | <p>(Cisco Unified Communications Manager only) Specifies the URL that Cisco IP Phone models 7940/7945/7960/7965/7970 use when the Directory button is pressed. This URL must return a CiscoIPPhoneMenu object even if no MenuItems are specified in the object. The MenuItems that are specified get appended to the directory list along with the three internal directories on the Cisco IP Phones.</p> <p>Maximum length: 255<br/>Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p>                                                                                                                           |
| URL Idle                         | <p>(Cisco Unified Communications Manager only) Specifies the URL that Cisco IP Phone models 7940, 7945, 7960, 7965, and 7970 use to display information on the screen when the phone remains idle for the time that the URL Idle Time parameter specifies.</p> <p>Maximum length: 255<br/>Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p>                                                                                                                                                                                                                                                                      |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL Idle Time          | <p>(Cisco Unified Communications Manager only) Specifies the time that the Cisco IP Phone models 7940, 7945, 7960, 7965, and 7970 should remain idle before displaying the URL that the URL Idle parameter specifies. If the time is set to zero, the URL that the URL Idle parameter specifies does not display.</p> <p>Default setting: 0<br/> Minimum: 0<br/> Maximum: 604800<br/> Unit: sec</p>                                                                                                                                                                                                                                            |
| URL Information        | <p>(Cisco Unified Communications Manager only) Specifies a URL that points to a page in the Cisco CallManager Cisco IP Phone (CCMCIP) webs and returns the requested help text to the Cisco IP phone models 7940, 7945, 7960, 7965, and 7970 display. This information displays when a user presses the i or ? button on the phones.</p> <p>Maximum length: 255<br/> Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p>                                                                                                               |
| URL Messages           | <p>(Cisco Unified Communications Manager only) Specifies a URL that the Cisco IP Phones should call when the Messages button is pressed. The URL must return a CiscoIPPhoneMenu object when called. The Menu Items that are returned get appended to the built-in items on Cisco IP Phone models 7940, 7945, 7960, 7965, and 7970.</p> <p>Maximum length: 255<br/> Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p>                                                                                                                 |
| IP Phone Proxy Address | <p>(Cisco Unified Communications Manager only) Specifies a proxy server name or address and port (for example, proxy.cisco.com:8080). If the proxy server is specified, the Cisco IP Phones use it to request all URLs. Leave this setting blank for the phones to attempt to connect directly to all URLs. If a name is used instead of an IP address, configure phones with valid DNS servers to allow name to IP resolution. Confirm that the proxy server is listening at the destination that is specified.</p> <p>Maximum length: 255<br/> Allowed values: Proxy server name or address and port (for example, proxy.cisco.com:8080)</p> |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL Services                           | <p>(Cisco Unified Communications Manager only) Specifies the URL that the Cisco IP phone models 7940, 7945, 7960, 7965, and 7970 call when the Services button is pressed. The initial request by the phone passes the device name as a parameter. The default page in the Cisco CallManager Cisco IP Phone (CCMCIP) web returns a CiscoIPPhoneMenu object with a list of services that are subscribed to the device. If no subscriptions exist, the return text indicates that no subscriptions exist for the device.</p> <p>Maximum length: 255<br/> Allowed values: A well-formed URL (for example, http://myserver/myscript.asp). Test the URL in a separate browser window to make sure that it is valid.</p> |
| <b>User Search Parameters</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Enable All User Search                 | <p>(Cisco Unified Communications Manager only) Determines whether to allow a search for All Users (search with no last name/first name/directory number specified) when searching for users via the Corporate Directory from the phone. This parameter also applies to the directory search on the Cisco CallManager User Options (CCMUser) window.</p> <p>This is a required field.<br/> Default setting: True</p>                                                                                                                                                                                                                                                                                                |
| User Search Limit                      | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of users to be retrieved from a search in the Corporate Directory feature on the phone. This parameter also applies to the directory search on the Cisco CallManager User Options (CCMUser) window. Using values greater than the default value (64) may negatively affect Cisco CallManager performance. Search does not apply when the Enable All User Search enterprise parameter is set to False and no criteria are set for the search.</p> <p>This is a required field.<br/> Default setting: 64<br/> Minimum: 1<br/> Maximum: 500</p>                                                                                           |
| <b>CCM Web Services Parameters</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Allowed Performance Queries per Minute | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of AVVID XML Layer (AXL) performance counter queries that are allowed per minute for the system. Clients such as Voice Health Monitoring and Gateway Statistic Utility (GSU) receive a slow response if applications send more queries than the limit that is imposed by this parameter.</p> <p>This is a required field.<br/> Default setting: 50<br/> Minimum: 1<br/> Maximum: 80</p>                                                                                                                                                                                                                                                |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allowed Device Queries per Minute                    | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of AVVID XML Layer (AXL) Device queries that are allowed per minute for the system. Clients such as Voice Health Monitoring and Gateway Statistic Utility (GSU) receive a slow response if applications send more queries than the limit that is imposed by this parameter.</p> <p>This is a required field.</p> <p>Default setting: 15<br/>Minimum: 1<br/>Maximum: 18</p> |
| Performance Queue Limit                              | <p>(Cisco Unified Communications Manager only) Controls the queue size that handles performance counter queries. If the queue size grows more than this limit, the performance request is dropped, and a timeout message is sent to the clients.</p> <p>This is a required field.</p> <p>Default setting: 100<br/>Minimum: 20<br/>Maximum: 1000</p>                                                                                                    |
| Maximum Performance Counters per Session             | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of performance counters that are allowed in a session-based request.</p> <p>This is a required field.</p> <p>Default setting: 100<br/>Minimum: 20<br/>Maximum: 1000</p>                                                                                                                                                                                                    |
| Allowed CDRonDemand get_file Queries per Minute      | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of CDRonDemand get_file queries that are allowed per minute for the system.</p> <p>This is a required field.</p> <p>Default setting: 10<br/>Minimum: 1<br/>Maximum: 20</p>                                                                                                                                                                                                 |
| Allowed CDRonDemand get_file_list Queries per Minute | <p>(Cisco Unified Communications Manager only) Specifies the maximum number of CDRonDemand get_file_list queries that are allowed per minute for the system.</p> <p>This is a required field.</p> <p>Default setting: 20<br/>Minimum: 1<br/>Maximum: 40</p>                                                                                                                                                                                            |
| <b>Trace Parameters</b>                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Close Thread Flag                                            | <p>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.</p> <p>This is a required field.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                  |
| FileCloseThreadQueueWater Mark                                    | <p>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.</p> <p>This is a required field.</p> <p>Default setting: 100<br/>Minimum: 0<br/>Maximum: 500</p>                                                                                                                                                        |
| <b>User Management Parameters</b>                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Effective Access Privileges for Overlapping User Groups and Roles | <p><i>(Cisco Unified Communications Manager only)</i> Determines the method for resolving overlapping resource privileges when a user is a member of more than one user groups and/or a group contains multiple roles. If set to maximum, the user is granted the highest privilege for the resources. If set to minimum, the user is granted the lowest privilege for the resources.</p> <p>This is a required field.</p> <p>Default setting: Maximum</p> |
| <b>Service Manager TCP Ports Parameters</b>                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Service Manager TCP Server Communication Port Number              | <p>Determines which TCP port number the Service Manager is listening to.</p> <p>This is a required field.</p> <p>Default setting: 8888<br/>Minimum: 1024<br/>Maximum: 65535</p>                                                                                                                                                                                                                                                                            |
| Service Manager TCP Client Communication Port Number              | <p>Determines which TCP port number the Service Manager responds to.</p> <p>This is a required field.</p> <p>Default setting: 8889<br/>Minimum: 1024<br/>Maximum: 65535</p>                                                                                                                                                                                                                                                                                |
| <b>CRS Application Parameters</b>                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Auto Attendant Installed                                          | <p><i>(Cisco Unified Communications Manager only)</i> <i>Display only.</i> Is true if the CRS Auto Attendant is installed and false otherwise. It can be modified only by CRS when it has been installed. If this flag is true, then the Auto Attendant information can be configured from the User Configuration page.</p> <p>This is a required field.</p> <p>Default setting: False</p>                                                                 |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPCC Express Installed                             | <p>(Cisco Unified Communications Manager only) Display only. Is true when a Cisco IPCC Express system is integrated with this Cisco CallManager cluster. It can be modified only by CRS when it has been installed. If this flag is true, then the IPCC Extension can be specified on the User Configuration page.</p> <p>This is a required field.</p> <p>Default setting: False</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Clusterwide Domain Configuration Parameters</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Organization Top Level Domain                      | <p>Defines the top level domain for the organization (for example, cisco.com).</p> <p>Maximum length: 255</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cluster Fully Qualified Domain Name                | <p>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.</p> <p>Maximum length: 255</p> <p>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.</p> |
| <b>Denial-of-Service Protection Parameters</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Denial-of-Service Protection Flag                  | <p>(Cisco Unified Communications Manager only) Enables protection used to thwart certain Denial-of-Service attacks.</p> <p>This is a required field.</p> <p>Default setting: True</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Cisco Support Use Parameters</b>                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Cisco Support Use 1                                | <p>Is used by Cisco TAC only.</p> <p>Maximum length: 10</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Cisco Syslog Agent Parameters</b>               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 37-1 Enterprise Parameter Descriptions (continued)**

| Enterprise Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Syslog Server Name                  | <p>Enter the name or IP address of the remote Syslog server that you want to use 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.</p> <p>Maximum length: 255<br/> Allowed values: Provide a valid remote syslog server name with the following characters: A-Z, a-z, 0-9, ., -</p> |
| Syslog Severity for Remote Syslog Messages | <p>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.</p> <p>This is a required field.<br/> Default setting: Error</p>                                                                                                                                                                                                            |
| <b>CUCReports Parameters</b>               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Report Socket Connection Timeout           | <p>Specifies the maximum number of seconds used when attempting to establish a connection with another server. Increase this time if connection issues are experienced on a slow network.</p> <p>This is a required field.<br/> Default setting: 10<br/> Minimum: 5<br/> Maximum: 120</p>                                                                                                                                                                                                                                                                    |
| Report Socket Read Timeout                 | <p>Specifies the maximum number of seconds used when reading data from another server. Increase this time if connection issues are experienced on a slow network.</p> <p>This is a required field.<br/> Default setting: 60<br/> Minimum: 5<br/> Maximum: 600</p>                                                                                                                                                                                                                                                                                            |



# CHAPTER 38

## Installing Plugins

---



### Caution

Information in this chapter is applicable in a standalone configuration only. If you have installed Cisco Unified Communications Manager Business Edition (CMBE), for information on installing plugins, see the *Cisco Unified Communications Manager Administration Guide* at [http://www.cisco.com/en/US/products/ps7273/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html).

---

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 click **Plugins**.
  - Step 2** On the Search Plugins page, click **Find**.
  - Step 3** For the plugin that you want to install, click **Download**.
  - Step 4** Follow the on-screen instructions for installing the plugin.
-





## CHAPTER 39

# Managing Descriptions of Message Attachments

---

When Cisco Unity Connection is integrated with a third-party message store, 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, page 39-1](#)
- [Changing a Description of a Message Attachment, page 39-2](#)
- [Deleting a Description of a Message Attachment, page 39-2](#)

## Adding a Description of a Message Attachment

### Revised May 2009

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

- 
- |               |                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In Cisco Unity Connection Administration, expand <b>System Settings</b> , then click <b>Attachment Descriptions</b> .                                                                                                                                                             |
| <b>Step 2</b> | On the Search TTS Descriptions of Message Attachments page, in the Language list, click the language for which you want to add a description of a message attachment.<br><br>Note that the list of languages depends on the languages (locales) that are installed on Connection. |
| <b>Step 3</b> | Click <b>Add New</b> .                                                                                                                                                                                                                                                            |
| <b>Step 4</b> | On the New TTS Description of Message Attachments page, enter a file extension in the File Extension field.<br><br>You must enter a period at the beginning of the file extension. Otherwise, you cannot add the description of the message attachment.                           |
| <b>Step 5</b> | In the Description field, enter the description that you want for the message attachment.                                                                                                                                                                                         |
| <b>Step 6</b> | Click <b>Save</b> .                                                                                                                                                                                                                                                               |
-

# Changing a Description of a Message Attachment

**Revised May 2009**

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 click **Attachment Descriptions**.
- Step 2** On the Search TTS Descriptions of Message Attachments page, in the Language list, click the language for which you want to change a description of a message attachment.
- Note that the list of languages depends on the languages (locales) that are installed on Connection.
- Step 3** In the Extension column, click 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** Click **Save**.
- 

# Deleting a Description of a Message Attachment

**Revised May 2009**

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 click **Attachment Descriptions**.
- Step 2** On the Search TTS Descriptions of Message Attachments page, in the Language list, click the language for which you want to delete a description of a message attachment.
- Note that the list of languages depends on the languages (locales) that are installed on Connection.
- Step 3** Check the check box next to the extension for the attachment description that you want to delete.
- Step 4** Click **Delete Selected**.
- Step 5** When prompted to confirm the deletion, click **OK**.
-



## CHAPTER 40

# Configuring Access to Emails in an External Message Store

---

See the following sections:

- [About User Access to Emails in an External Message Store, page 40-1](#)
- [Configuring Access to Emails in an Exchange 2007 Message Store, page 40-1](#)
- [Configuring Access to Emails in an Exchange 2003 Message Store, page 40-5](#)

## About User Access to Emails in an External Message Store

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 log on 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.

## Configuring Access to Emails in an Exchange 2007 Message Store

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 Offering Users Access to Exchange 2007 Emails, page 40-2](#)
- [Enabling IMAP Access to Exchange, page 40-2](#)
- [Configuring Secure IMAP with SSL and Enabling the SSL Certificate \(Exchange 2007 Only\), page 40-3](#)
- [Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access, page 40-4](#)
- [Configuring Users for the External Services, page 40-5](#)

## Task List for Offering Users Access to Exchange 2007 Emails

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”](#) section on page 40-2.
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 \(Exchange 2007 Only\)”](#) section on page 40-3.
3. Create Connection external services. See the [“Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access”](#) section on page 40-4.
4. Configure the users for the external services. See the [“Configuring Users for the External Services”](#) section on page 40-5.
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 Connection that specifies the Exchange server on which the mailbox for the user is stored. This enables users to access their email when they log on to Connection by phone.

## Enabling IMAP Access to Exchange

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 Connection users to be able to access.

### To Enable IMAP Access to Exchange

- 
- |               |                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | On an Exchange server that contains emails that you want licensed Connection users to be able to access, log on to Windows by using an account that is a member of the local Administrators group.                                     |
| <b>Step 2</b> | On the Windows Start menu, click <b>Administrative Tools &gt; Services</b> .                                                                                                                                                           |
| <b>Step 3</b> | In the right pane, find the <b>Microsoft Exchange IMAP4</b> service.                                                                                                                                                                   |
| <b>Step 4</b> | If the value of the Status column is <b>Started</b> and the value of the Startup Type column is <b>Automatic</b> , skip to <a href="#">Step 9</a> .<br><br>If the values are different, double-click <b>Microsoft Exchange IMAP4</b> . |
| <b>Step 5</b> | In the Microsoft Exchange IMAP4 Properties dialog box, if Startup Type is not Automatic, change it to <b>Automatic</b> .                                                                                                               |
| <b>Step 6</b> | If Service Status is not Started, click <b>Start</b> .                                                                                                                                                                                 |
| <b>Step 7</b> | Click <b>OK</b> to close the Microsoft Exchange IMAP4 Properties dialog box.                                                                                                                                                           |
| <b>Step 8</b> | Close the Services MMC.                                                                                                                                                                                                                |
| <b>Step 9</b> | Repeat <a href="#">Step 1</a> through <a href="#">Step 8</a> on each Exchange server that contains emails that you want licensed Connection users to be able to access.                                                                |
-

## Configuring Secure IMAP with SSL and Enabling the SSL Certificate (Exchange 2007 Only)

### To Configure Secure IMAP with SSL and Enable the SSL Certificate (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 choose 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 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 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 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 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”](#) section on page 40-4. 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 click **Properties**.
 - Step 15** In the Properties dialog box, click the **Directory Security** tab.
 - Step 16** Under Secure Communications, click **Edit**.
 - Step 17** Check the **Require Secure Channel** check box.
 - Step 18** Click **OK**.
 - Step 19** In the Properties dialog box, click **OK**.
-

Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails

- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
 - Step 2** On the Search External Services page, click **Add New**.
 - Step 3** On the New External Service page, in the Type list, click **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 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 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, click **NTLM**.
 - Step 8** In the Security Transport Type list, if you created and installed SSL certificates, click **SSL**. Otherwise, click **None**.
 - Step 9** If you selected SSL in [Step 8](#), check the **Validate Server Certificates** check box. Otherwise, skip to [Step 10](#).
 - Step 10** Under Service Capabilities, check the **User Access to Email in Third-Party Message Store** check box.
 - Step 11** Click **Save**.
 - Step 12** Repeat [Step 2](#) through [Step 13](#) for each additional Exchange 2007 server that contains emails that you want licensed Connection users to access.
 - Step 13** Close Cisco Unity Connection Administration.
-

Configuring Users for the External Services

Do the following procedure.

**Note**

Exchange must have a user for each Connection user that you are configuring.

To Configure Users for the External Services

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**.
- Step 5** On the New External Service Accounts page, in the External Service field, click 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”](#) section on page 40-4.
- Step 6** In the Email Address field, enter the email address for the user.
- Step 7** In the Login Type field, click the applicable option:
 - **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2007 is the same as the Connection user alias. Connection will log on the user with the 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 Connection user alias). Connection will log on 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. Connection will log on 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** Click **Save**.
- Step 12** To check the Exchange configuration for the user, click **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 Access to Emails in an Exchange 2003 Message Store

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 Offering Users Access to Exchange 2003 Emails](#), page 40-6
- [Enabling IMAP Access to Exchange](#), page 40-7
- [Creating and Configuring an Active Directory Service Account \(Exchange 2003 Only\)](#), page 40-7
- [Creating and Installing SSL Certificates \(Exchange 2003 Only\)](#), page 40-8
- [Requiring Secure Communication Between Cisco Unity Connection and Exchange \(Exchange 2003 Only\)](#), page 40-12
- [Configuring the Cisco Unity Connection Server to Trust Exchange Certificates \(Exchange 2003 Only\)](#), page 40-13
- [Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access](#), page 40-15
- [Configuring Users for the External Services](#), page 40-15

Task List for Offering Users Access to Exchange 2003 Emails

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”](#) section on page 40-7.
2. Create an Active Directory service account that Connection uses to access Exchange data, and grant the account the necessary permissions. See the [“Creating and Configuring an Active Directory Service Account \(Exchange 2003 Only\)”](#) section on page 40-7.
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 \(Exchange 2003 Only\)”](#) section on page 40-8.
4. *(Optional but recommended)* Configure IIS to refuse unencrypted communications from web clients including Connection. See the [“Requiring Secure Communication Between Cisco Unity Connection and Exchange \(Exchange 2003 Only\)”](#) section on page 40-12.
5. Configure 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 \(Exchange 2003 Only\)”](#) section on page 40-13.
6. Create Connection external services. See the [“Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access”](#) section on page 40-15.
7. Configure the users for the external services. See the [“Configuring Users for the External Services”](#) section on page 40-15.
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 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 log on to Connection by phone.

Enabling IMAP Access to Exchange

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 Connection users to be able to listen to by using TTS.

To Enable IMAP Access to Exchange

-
- Step 1** On an Exchange server that contains emails that you want licensed Connection users to be able to access, log on to Windows by using an account that is a member of the local Administrators group.
 - Step 2** On the Windows Start menu, click **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, click **Start**.
 - Step 7** Click **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 Connection users to be able to access.
-

Creating and Configuring an Active Directory Service Account (Exchange 2003 Only)

Cisco Unity Connection accesses Exchange 2003 email by using an Active Directory account that acts as a proxy for 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

-
- Step 1** On a computer on which Active Directory Users and Computers and Exchange System Manager are installed, log on to Windows by using an account that is a member of the Domain Administrators group.
 - Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers**.
 - Step 3** In the left pane, expand **<Server name>**, right-click **Users**, and click **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, click **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 click **Properties**.
- Step 8** In the <Server name> Properties dialog box, click the **Security** tab.
- Step 9** Click **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** Click **Check Names**.
- Step 12** Click **OK** to close the dialog box.
- Step 13** In the <Server name> Properties dialog box, in the Group or User Names list, click the name of the service account.
- Step 14** In the Permissions For <Account name> list, set the permissions:
- For Full Control, check the **Deny** check box.
 - For Receive As, check the **Allow** check box
- Step 15** Click **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 (Exchange 2003 Only)

In this section, you create and install an SSL certificate on each Exchange server that contains emails that you want licensed 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 \(Exchange 2003 Only\)”](#) section on page 40-7 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 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”](#) procedure on page 40-9.
- An external certification authority—skip to the [“To Create a Certificate Signing Request”](#) procedure on page 40-9.

To Install the Microsoft Certificate Services Component

- 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** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 3** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.

- Step 4** In the left pane of the Add or Remove Programs control panel, click **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, click **Yes**.
- Step 7** Click **Next**.
- Step 8** On the CA Type page, click **Stand-alone Root CA**, and click **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** Click **Next**.
- Step 13** On the Certificate Database Settings page, click **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, click **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, click **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 Connection users to be able to access.

To Create a Certificate Signing Request

-
- Step 1** On a server on which Exchange System Manager is installed, log on to Windows by using an account that is an Exchange Full Administrator.
 - Step 2** On the Windows Start menu, click **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 Connection users to be able to access.
 - Step 4** Right-click **Default IMAP4 Virtual Server**, and click **Properties**.
 - Step 5** In the Properties dialog box, click the **Access** tab.
 - Step 6** Click **Certificate**.
 - Step 7** On the Welcome to the Web Server Certificate Wizard page, click **Next**.
 - Step 8** On the Server Certificate page, click **Create a New Certificate**.
 - Step 9** Click **Next**.
 - Step 10** On the Delayed or Immediate Request page, click **Prepare the Request Now But Send It Later**.

- Step 11** Click **Next**.
- Step 12** On the Name and Security Settings page, enter a name for the certificate (for example, <Server name>_Cert).
- Step 13** Click **Next**.
- Step 14** On the Organization Information page, enter the applicable values.
- Step 15** Click **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 connection.

- Step 17** Click **Next**.
- Step 18** On the Geographical Information page, enter the applicable information.
- Step 19** Click **Next**.
- Step 20** On the Certificate Request File Name page, enter a path and file name, 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” procedure on page 40-8](#), try to choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.
- Step 21** Click **Next**.
- Step 22** On the Request File Summary page, click **Next**.
- Step 23** On the Completing the Web Server Certificate Wizard page, click **Finish**.
- Step 24** Click **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 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” procedure on page 40-12](#).

Issue certificates or have them issued for each of the certificate signing requests that you created in the [“To Create a Certificate Signing Request” procedure on page 40-9](#):

- 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” procedure on page 40-12](#).
- 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” procedure on page 40-12](#).

To Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

-
- Step 1** On the server on which you installed Microsoft Certificate Services, log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **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 40-8](#).
- Step 4** Right-click the name of the certification authority, and click **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” procedure on page 40-9](#), and double-click the file.
- Step 6** In the left pane of Certification Authority, click **Pending Requests**.
- Step 7** Right-click on the pending request that you submitted in [Step 5](#), and click **All Tasks > Issue**.
- Step 8** In the left pane of Certification Authority, click **Issued Certificates**.
- Step 9** Right-click the new certificate, and click **All Tasks > Export Binary Data**.
- Step 10** In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, click **Binary Certificate**.
- Step 11** Click **Save Binary Data to a File**.
- Step 12** Click **OK**.
- Step 13** In the Save Binary Data dialog box, enter a path and file name, 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 choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.
- Step 14** Click **OK**.
- Step 15** If you created more than one certificate signing request in the [“To Create a Certificate Signing Request” procedure on page 40-9](#), 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 Connection users to be able to access.

To Install the Server Certificate

-
- Step 1** On a computer on which Exchange System Manager is installed, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **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 Connection users to be able to access.
- Step 4** Right-click **Default IMAP4 Virtual Server**, and click **Properties**.
- Step 5** Click the **Access** tab.
- Step 6** Click **Certificate**.
- Step 7** On the Welcome to the Web Server Certificate Wizard, click **Next**.
- Step 8** On the Pending Certificate Request page, click **Process the Pending Request and Install the Certificate**.
- Step 9** Click **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** Click **Next**.
- Step 12** On the Certificate Summary page, click **Next**.
- Step 13** On the Completing the Web Server Certificate Wizard page, click **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 (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 Connection users to be able to access, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **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 click **Properties**.
- Step 5** Click the **Access** tab.
- Step 6** Click **Communication**.
- Step 7** Click **Require Secure Channel**.
- Step 8** Click **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, click the **Stop** icon.
- Step 12** Wait a few seconds.
- Step 13** Click the **Play** icon.
- Step 14** Repeat [Step 1](#) through [Step 13](#) for each additional Exchange server that contains emails that you want licensed Connection users to be able to access.
-

Configuring the Cisco Unity Connection Server to Trust Exchange Certificates (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 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 Connection server.
- Step 2** On the server on which you installed Microsoft Certificate Services, log on to Windows by using an account that is a member of the local Administrators group.
- Step 3** On the Windows Start menu, click **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 click **Properties**.

- Step 6** In the <Certification authority name> Properties dialog box, on the **General** tab, in the CA Certificates list, click the name of one of the certificates that you issued for the Exchange servers.
- Step 7** Click **View Certificate**.
- Step 8** In the Certificate dialog box, click the **Details** tab.
- Step 9** Click **Copy to File**.
- Step 10** On the Welcome to the Certificate Export Wizard page, click **Next**.
- Step 11** On the Export File Format page, click **Base-64 Encoded X.509 (.CER)**.
- Step 12** Click **Next**.
- Step 13** On the File to Export page, enter a temporary path and file name 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 Connection server.

- Step 14** Write down the path and file name because you will need it later in this procedure.
- Step 15** Click **Next**.
- Step 16** On the Completing the Certificate Export Wizard page, click **Finish**.
- Step 17** Click **OK** to close the “Export successful” message box.
- Step 18** Click **OK** to close the Certificate dialog box.
- Step 19** Click **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 Connection server.
- Step 22** On the Connection server, log on to Cisco Unified Operating System Administration.
- Step 23** On the Security menu, click **Certificate Management**.
- Step 24** On the Certificate List page, click **Upload Certificate**.
- Step 25** On the Upload Certificate page, in the Certificate Name list, click **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** Click **Browse**.
- Step 28** In the Choose File dialog box, browse to the location of the certificate file, click the name of the file, and click **Open**.
- Step 29** On the Upload Certificate page, click **Upload File**.
- Step 30** When the Status area reports that the upload succeeded, click **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 Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
 - Step 2** On the Search External Services page, click **Add New**.
 - Step 3** On the New External Service page, in the Type list, click **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 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 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](#)” procedure on page 40-9.
 - Step 7** In the Authentication Mode list, click **NTLM**.
 - Step 8** In the Security Transport Type list, if you created and installed SSL certificates, click **SSL**. Otherwise, click **None**.
 - Step 9** If you selected SSL in [Step 8](#), check the **Validate Server Certificates** check box. Otherwise, continue to [Step 10](#).
 - Step 10** Under Service Credentials, in the Alias field, enter the Active Directory user logon name of the service account that you created in the “[To Create and Configure a Service Account That Can Access Exchange Emails](#)” procedure on page 40-7. 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** Click **Save**.
 - Step 14** Repeat [Step 2](#) through [Step 13](#) for each additional Exchange server that contains emails that you want licensed Connection users to be able to access.
 - Step 15** Close Cisco Unity Connection Administration.
-

Configuring Users for the External Services

Do the following procedure.

**Note**

Exchange must have a user for each Connection user that you are configuring.

To Configure Users for the External Services

-
- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, click the alias of a user.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click **Add New**.
- Step 5** On the New External Service Accounts page, in the External Service field, click 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”](#) section on page 40-15.
- Step 6** In the Email Address field, enter the email address for the user.
- Step 7** In the Login Type field, click the applicable option:
- **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2003 is the same as the Connection user alias. Connection will log on the user with the 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 Connection user alias). Connection will log on 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** Click **Save**.
- Step 11** To check the Exchange configuration for the user, click **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.
-



CHAPTER 41

Generating Reports

You can use Cisco Unity Connection reports to gather information about system configuration and call handlers. See the following sections:

- [Reports Overview, page 41-1](#)
- [Setting Report Configuration Parameters, page 41-4](#)
- [Generating and Viewing Reports, page 41-5](#)

Reports Overview

Revised May 2009

You can generate the following reports in Cisco Unity Connection Administration:

Table 41-1 **System Configuration and Call Management Reports**

Report Name	Description of Output
Phone Interface Failed Logon	Output includes the following information for every failed attempt to log on to Connection by phone: <ul style="list-style-type: none">• User name, alias, caller ID, and extension of the user who failed to log on.• Date and time that the failed logon occurred.• Whether the maximum number of failed logons has been reached for the user.
Users	Output includes the following information for each user: <ul style="list-style-type: none">• Last name, first name, and alias.• Information that identifies the Connection server associated with the user.• Billing ID, class of service, and extension.• Whether the user has enabled personal call transfer rules.

Table 41-1 **System Configuration and Call Management Reports (continued)**

Report Name	Description of Output
Message Traffic	<p>Output includes totals for the following traffic categories:</p> <ul style="list-style-type: none"> • Voice. • Fax. • Email. • NDR. • Delivery. • Read receipt. • Hourly totals. • Daily totals.
Port Activity	<p>Output includes the following information for voice messaging ports:</p> <ul style="list-style-type: none"> • Name. • Number of inbound calls handled. • Number of outbound MWI calls handled. • Number of outbound AMIS calls handled. • Number of outbound notification calls handled. • Number of outbound TRaP calls handled. • Total number of calls handled. • Total number of ports.
Subscriber Message Activity	<p>Output includes the following information about messages sent and received, per user:</p> <ul style="list-style-type: none"> • Name, extension, and class of service. • Date and time for each message. • Information on the source of each message. • Action completed (for example, new message, message saved, MWI On requested, and so on). • Information on the number of new messages received for a user, and on the message sender. • Dial out number and results.
Distribution Lists	<p>Output includes the following information:</p> <ul style="list-style-type: none"> • Name and display name of the list. • Date and time the list was created. • Date and time of the creation of the distribution list is given in Greenwich mean time. • A count of the number of users included in the list. • If the Include List Members check box is checked, a listing of the alias of each user who is a member of the list.

Table 41-1 **System Configuration and Call Management Reports (continued)**

Report Name	Description of Output
User Lockout	<p>Output includes user alias, the number of failed logon attempts for the user, credential type (a result of “4” indicates a logon attempt from the Connection conversation; a result of “3” indicates a logon attempt from a web application) and the date and time that the account was locked.</p> <p>Note Date and time of the lockout of the user account is given in Greenwich mean time.</p>
Unused Voice Mail Accounts	<p>Output includes user alias and display name, and the date and time that the user account was created.</p> <p>Note Date and time of the creation of the user account is given in Greenwich mean time.</p>
Transfer Call Billing	<p>Output includes the following information for each call:</p> <ul style="list-style-type: none"> • Name, extension, and billing ID of the user. • Date and time that the call occurred. • The phone number dialed. • The result of the transfer (connected, ring-no-answer (RNA), busy, or unknown).
Outcall Billing Detail	<p>Output includes the following information, arranged by day and by the extension of the user who placed the call:</p> <ul style="list-style-type: none"> • Name, extension, and billing ID. • Date and time the call was placed. • The phone number called. • The result of the call (connected, ring-no-answer (RNA), busy, or unknown). • The duration of the call in seconds.
Outcall Billing Summary	<p>Output is 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.</p>
Call Handler Traffic	<p>Output includes the following information for each call handler, in rows for each hour of a day:</p> <ul style="list-style-type: none"> • Total number of calls. • Number of times each phone keypad key was pressed. • Extension. • Invalid extension. • Number of times the after greeting action occurred. • Number of times the caller hung up.
System Configuration	<p>Output includes detailed information about all aspects of the configuration of the Connection system.</p>

Table 41-1 **System Configuration and Call Management Reports (continued)**

Report Name	Description of Output
Mailbox Store	<p>Includes the following information about the specified mailbox stores:</p> <ul style="list-style-type: none"> • Mail database name. • Display name. • Server name. • Whether access is enabled. • Mailbox store size. • Number of Mailboxes. • Last error. • Status. • Maximum size before warning. • Whether the mail database can be deleted.
Dial Plan	<p>Includes a list of the search spaces that are configured on the Connection or Cisco Unified CMBE server, with an ordered list of partitions assigned to each search space.</p> <p>If the server is part of a Digital Network, the report also lists the search spaces and associated partition membership on every other Connection location on the network.</p>
Dial Search Scope	<p>Includes a list of all users and their extensions in the specified partition that is configured in the Connection directory. If a partition is not specified, the report lists all users and their extensions for all partitions that are configured in the directory.</p>

Setting Report Configuration Parameters

Revised May 2009

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 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 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

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, click **Cisco Unity Connection Serviceability** and click **Go**.

For details on generating and viewing reports for Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.



CHAPTER 42

Configuring and Customizing a Cisco Unity Connection Cluster

You can configure a Cisco Unity Connection cluster by using the Find and List Servers and Server Configuration pages. These pages are available in Cisco Unity Connection Administration by expanding System Settings, then clicking Cluster.

You can customize the Connection cluster settings by using the Cluster Configuration page. This page is available in Connection Administration by expanding System Settings, then clicking Advanced > Cluster Configuration.

For the applicable procedures, see the “[Configuring a Cisco Unity Connection Cluster](#)” chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*.



Note

The Connection cluster feature is not supported for use with Cisco Unified Communications Manager Business Edition.



CHAPTER 43

Integrating Cisco Unity Connection 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 Connection users by importing user data from the LDAP directory, and
- Configure Connection to periodically resynchronize Connection data with data in the LDAP directory.

For a list of the LDAP directories that are supported for use with Connection, see the “Requirements for an LDAP Directory Integration” section in *System Requirements for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.

Note that you can only use the information in this chapter to integrate Cisco Unity Connection with an LDAP directory. For information on integrating Cisco Unified Communications Manager Business Edition with an LDAP directory, see the following documentation available at http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html:

- The “Understanding the Directory” chapter of the *Cisco Unified Communications Manager System Guide for Cisco Unified Communications Manager Business Edition*.
- The “End User Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*.

See the following sections:

- [Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users](#), page 43-2
- [Activating the Cisco DirSync Service](#), page 43-3
- [Enabling LDAP Synchronization](#), page 43-3
- [Converting Phone Numbers into Extensions](#), page 43-4
- [Uploading SSL Certificates on the Connection Server](#), page 43-4
- [Configuring LDAP Authentication](#), page 43-5
- [Filtering LDAP Users](#), page 43-6
- [Adding LDAP Configurations and Synchronizing Data](#), page 43-7

Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users

To configure LDAP and to create users by importing user data from the LDAP directory, do the following tasks:

1. Activate the Cisco DirSync service. See the [“Activating the Cisco DirSync Service”](#) section on page 43-3.
2. Enable LDAP synchronization. See the [“Enabling LDAP Synchronization”](#) section on page 43-3.
If you are using LDAP authentication to authenticate user access to Connection web applications or IMAP access to 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 Connection, specify a filter that converts phone numbers into extensions when you import LDAP data into Connection. See the [“Converting Phone Numbers into Extensions”](#) section on page 43-4.

(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 8., 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 43-4.)



Note To integrate existing Connection users with LDAP users, you must use BAT.

4. (Optional) If you want to use SSL to encrypt the user names 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 Connection server during synchronization, export an SSL certificate from the applicable LDAP servers and upload the certificates on all Connection servers. See the [“Uploading SSL Certificates on the Connection Server”](#) section on page 43-4.
5. (Optional) If you want Connection users who access a Connection web application or who access Connection voice messages by using an IMAP email application to authenticate their user name and password against the LDAP directory, configure LDAP authentication. See the [“Configuring LDAP Authentication”](#) section on page 43-5.
6. (Optional) If user search bases do not give you enough control over which LDAP users are synchronized with Connection users, you may want to specify an LDAP filter. See the [“Filtering LDAP Users”](#) section on page 43-6.
7. Add one or more LDAP configurations, which define the LDAP directory and user search bases in which Connection accesses data, and synchronize the Cisco Unified Communications Manager directory with the LDAP directory. See the [“Adding LDAP Configurations and Synchronizing Data”](#) section on page 43-7.
8. If you are synchronizing existing Connection users with users in an LDAP directory, do the procedure in the [“Integrating Existing Cisco Unity Connection User Accounts with LDAP User Accounts”](#) section in the “Creating User Accounts from LDAP User Data” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

If you are creating new 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 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 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

The Cisco DirSync service must be activated for Connection to access an LDAP directory. Do the following procedure.

To Activate the Cisco DirSync Service

-
- Step 1** Log on to Cisco Unified Serviceability as a user that has the System Administrator role.
 - Step 2** On the Tools menu, click **Service Activation**.
 - Step 3** Under Directory Services, check the **Cisco DirSync Service** check box.
 - Step 4** Click **Save**, and click **OK** to confirm.
-

Enabling LDAP Synchronization

LDAP synchronization must be enabled for Connection to access an LDAP directory. Do the following procedure.

To Enable LDAP Synchronization

-
- Step 1** Log on to Cisco Unity Connection Administration as a user that has the System Administrator role.
 - Step 2** Expand **System Settings > LDAP**, then click **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, choose the type of LDAP server that you want to access.
 - Step 5** In the LDAP Attribute for User ID list, choose the field in the LDAP directory whose data you want to appear in the Alias field in Connection. The field that you choose must have a value for every user in the LDAP directory. In addition, every value for that field must be unique.



Caution

If you later need to change the field that you choose now, and if you have already created LDAP configurations on the LDAP Directory page, you must delete all LDAP configurations, change the value here, and recreate all LDAP configurations.

-
- Step 6** Click **Save**.
-

Converting Phone Numbers into Extensions

If you want to map phone numbers in the LDAP directory to extensions in Connection but the phone numbers do not match the extensions, you can add a regular expression that converts the phone numbers into extensions.



Note

A regular expression may not be sufficient to convert phone numbers in your LDAP directory into Connection extensions. In that case, 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 Connection users from LDAP data by using the Bulk Administration Tool or synchronize existing Connection users with LDAP users, also by using the Bulk Administration Tool, you can manipulate phone number data in the CSV file using a spreadsheet application before you import the data back into Connection. See either the [“Creating Cisco Unity Connection Users from LDAP Data by Using the Bulk Administration Tool”](#) or the [“Integrating Existing Cisco Unity Connection User Accounts with LDAP User Accounts”](#) section, as applicable, in the “Creating User Accounts from LDAP User Data” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

To Add a Filter That Converts LDAP Phone Numbers into Cisco Unity Connection Extensions

- Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then click **Advanced LDAP Settings**.
- Step 2** In the Filter to Convert LDAP Phone Numbers into Connection Extensions field, enter a regular expression to convert the phone number that is imported from the LDAP directory into an extension for use in Connection. For example:
 - To use the phone number as the extension, without punctuation, if any, enter:
[0-9]+
 - To use the last four digits of the phone number as the extension, enter:
[0-9][0-9][0-9][0-9]\$
 - To use the first four digits of the phone number as the extension, enter:
^[0-9][0-9][0-9][0-9]

For more information on regular expressions, do a web search on “regular expression.”
- Step 3** Click **Save**.

Uploading SSL Certificates on the Connection Server

Added May 2009

If you want to use SSL to encrypt data that is transmitted between the LDAP server and the 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 Configurations and Synchronizing Data” section on page 43-7](#)), or for authentication (see the [“Configuring LDAP Authentication” section on page 43-5](#)).

To Upload SSL Certificates from the LDAP Directory Servers

Step 1 Export the SSL certificate from the LDAP server with which you want Connection to synchronize data and from the LDAP server that you want Connection to access when authenticating user logons, 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 Connection to synchronize or authenticate.

Step 2 On the Connection server, log on to Cisco Unified Operating System Administration.

Step 3 On the Security menu, click **Certificate Management**.

Step 4 Upload the directory certificate trust that you exported in [Step 1](#).

If you want this 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, click **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 Connection clustering, or if you are configuring a Digital Network, repeat [Step 2](#) through [Step 4](#) on the other Connection servers.

Configuring LDAP Authentication

Revised May 2009

If you want to use LDAP user names and passwords to authenticate logons to Cisco Unity Connection web applications or IMAP access to Connection voice messages, do the following procedure to configure LDAP authentication.

To Configure LDAP Authentication

Step 1 In Cisco Unity Connection Administration, expand **System Settings > LDAP**, and click **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, click **This Page**.

If you uploaded SSL certificates to the Connection server in the [“To Upload SSL Certificates from the LDAP Directory Servers” procedure on page 43-5](#):

- 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), 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 Connection allows you to specify redundant servers, see the “[Requirements for an LDAP Directory Integration](#)” section in *System Requirements for Cisco Unity Connection Release 7.x*.

Step 4 Click **Save**.

Filtering LDAP Users

Added May 2009

**Note**

This feature was added for Cisco Unity Connection 7.0(2).

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 Connection users.
- The LDAP directory structure does not match the way you want to import users into Connection. For example:
 - If organizational units are set up according to an organizational hierarchy but users are mapped to 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 Connection server, you need to do something to prevent users from having mailboxes on more than one Connection server.

In these cases, you may want to use the “set cuc ldapfilter” CLI command to provide additional control over user search bases. Note the following:

- The “set cuc ldapfilter” CLI command cannot be used with Cisco Unified Communications Manager Business Edition.
- You can only create one filter per Connection server or Connection cluster pair, so the LDAP filter must specify all of the users that you want to synchronize with Connection users.
- When you configure LDAP synchronization in Connection, you can further filter the LDAP users by your choice of user search bases.
- The filter must adhere to the LDAP filter syntax specified in RFC 2254, “The String Representation of LDAP Search Filters.”

- The filter syntax is not verified, and no error message is returned. We recommend that you verify the LDAP filter syntax before you include it in this command.
- After you run this command, you must do the following steps for the LDAP users specified by the filter to be accessible to Connection:
 1. Deactivate and reactivate the Cisco DirSync service. In Cisco Unified Serviceability, click Tools > Service Activation. Uncheck the check box next to Cisco DirSync, and click Save to deactivate the service. Then check the check box next to Cisco DirSync, and click Save to reactivate the service.
 2. Perform a full synchronization in Connection Administration.
- If you re-run this command and specify a filter that excludes some of the users who were accessible with the previous filter, the Connection users who are synchronized with the now-inaccessible LDAP users will be converted to standalone Connection users over the next two scheduled synchronizations or within 24 hours, whichever is greater. The users will still be able to log on to Connection by phone, callers can still leave messages for them, and their messages will not be deleted. However, they will not be able to log on to Connection web applications while 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 Connection accounts were created.

Adding LDAP Configurations and Synchronizing Data

Revised May 2010

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.



Note

If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; 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 Connection Alias field; the UPN is guaranteed by Active Directory to be unique across the forest.

To Add an LDAP Configuration

- Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then click **LDAP Directory Configuration**.
- Step 2** In the LDAP Configuration Name field, enter a name for this LDAP configuration. If you are adding several LDAP configurations 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, see the “[LDAP Directory Configuration](#)” section in the “System Settings” chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 7.x*.

If you uploaded SSL certificates to the Connection server in the “[To Upload SSL Certificates from the LDAP Directory Servers](#)” procedure on page 43-5, 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 Connection allows you to specify redundant servers, see the “[Requirements for an LDAP Directory Integration](#)” section in *System Requirements for Cisco Unity Connection Release 7.x*.

Step 4 Click **Save**.

Step 5 To add another LDAP configuration for another user search base, click **Add New**, and repeat [Step 2](#) through [Step 4](#).

When you have added the last LDAP configuration, continue with [Step 6](#).

Step 6 Click **Perform Full Sync Now**.



CHAPTER 44

Managing Licenses

See the following sections:

- [About License Files, page 44-1](#)
- [Obtaining and Installing a License File, page 44-2](#)
- [Viewing Reports for Licenses, page 44-4](#)
- [License Parameters for Cisco Unity Connection Features, page 44-6](#)

About License Files

Added May 2009

See the following sections:

- [License Files and MAC Addresses, page 44-1](#)
- [Cisco Unity Connection Can Use Multiple Installed License Files, page 44-2](#)
- [License Files Must Be Installed, page 44-2](#)
- [Permanent, Time-Expiring, and Demonstration License Files, page 44-2](#)
- [License Files and Cisco Unity Connection Clusters, page 44-2](#)

License Files and MAC Addresses

Each license file (except for the demonstration license file) is registered to the MAC address of the network interface card (NIC) on the Cisco Unity Connection server. The license file for one server cannot be used on a second server (for example, because you want to replace the Connection server). You must obtain a replacement license file that is registered to the MAC address on the second server.

The license file can be registered to only one MAC address. If the Connection server has a dual NIC, you must either configure it for network fault tolerance, which assigns one MAC address to both NICs, or disable one of the NICs and use the MAC address for the other NIC.

When you order a license file for a dual NIC that has been configured for network fault tolerance, specify the virtual MAC address that applies to both NICs rather than the physical MAC address for either of the NICs. The license file is registered to the virtual MAC address, so the license will continue to be valid even if one of the NICs fails.

Cisco Unity Connection Can Use Multiple Installed License Files

Multiple license files can be installed on a Cisco Unity Connection server. Each installed license file may enable one or more features. All of the installed license files combined enable the features that the customer wants.

Before a license file can be installed, it must be added to the Licenses page in Cisco Unity Connection Administration.

Note that if the Connection demonstration license is installed on the Connection server, it must be the only license file that is installed, even though you may have added other license files.

License Files Must Be Installed

For license files to become effective, they must be installed after they are added to the Licenses page. For details on installing license files, see the [“To Install the License Files” procedure on page 44-3](#).

Permanent, Time-Expiring, and Demonstration License Files

The following types of license files are available:

- Permanent license files are registered to the MAC address of the network interface card (NIC) on the Cisco Unity Connection server. These license files do not have an expiration date.
- Time-expiring license files are registered to the MAC address of the NIC on the Connection server. These license files have an expiration date. All of the features that are enabled by a time-expiring license file will be disabled after the expiration date.
- Demonstration license files are not registered to a MAC address. These license files do not have an expiration date and enable only a limited range of features (for example, a maximum of two voice messaging ports and ten users with voice mailboxes). A demonstration license file is included with every Connection server. If this license file is installed, it must be the only license file that is installed on the Connection server.

For information on obtaining and installing license files, see the [“Obtaining and Installing a License File” section on page 44-2](#).

License Files and Cisco Unity Connection Clusters

When a Cisco Unity Connection cluster (high availability) is configured, two licenses are required. The license that has the MAC address of the publisher server must be installed on the publisher server. The license that has the MAC address of the subscriber server must be installed on the subscriber server. For details on installing license files, see the [“To Install the License Files” procedure on page 44-3](#).

Obtaining and Installing a License File

Revised May 2009

License files, which enable the features purchased by the customer, are required for configuring a new Cisco Unity Connection system and for adding or changing licensed features. You obtain the license files by completing registration information on Cisco.com.

**Note**

When a Cisco Unity Connection cluster (high availability) is configured, two licenses are required. The license that has the MAC address of the publisher server must be installed on the publisher server. The license that has the MAC address of the subscriber server must be installed on the subscriber server.

Shortly after registration, Cisco emails the license files. The email from Cisco contains instructions on how to save and store the files.

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity Connection server.
- The product authorization key (PAK), which appears on the sticker located on the back of the Cisco Unity Connection Application Software Media kit.

This section contains three procedures. Do them in the order listed. For a Cisco Unity Connection cluster, you must do all three procedures on each Connection server in the cluster.

To Get the MAC Address of the Cisco Unity Connection Server

-
- Step 1** Log on to Cisco Unified Communications Operating System Administration.
- Step 2** On the Show menu, click **Network**.
- Step 3** Write down the value for MAC Address, excluding the hyphens (for example, if the physical address is 00-a1-b2-c3-d4-e5, record 00a1b2c3d4e5), or save it to a file that you can access during online registration.
-

To Register and Obtain the License Files

-
- Step 1** Go to the software registration site at <http://www.cisco.com/go/license> (URLs are case sensitive; you may be required to log on).
- Step 2** Enter the PAK and click **Submit**.
- Step 3** Follow the on-screen prompts.
- Step 4** You will receive an email with the Cisco Unity Connection license file.
-

To Install the License Files

-
- Step 1** If Cisco Unity Connection is not configured for a cluster, in Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- If a Connection cluster is configured, on the publisher server, in Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 2** On the Search License page, click **Add New**.
- Step 3** On the Add New License page, click **Browse**, and locate the new license file.
- Step 4** If Connection is not configured for a cluster, in the Choose File dialog box, double-click the name of the license file.

If a Connection cluster is configured, in the Choose File dialog box, double-click the name of the license file that has the MAC address of the publisher server.

**Caution**

If you rename the license file, the file name can contain alphanumeric characters, hyphens, and underscores, but must start with an alphabetic character. Otherwise, the license file cannot be installed.

- Step 5** On the Add New License page, click **Add**.
- Step 6** If you have more than one new license file, repeat [Step 2](#) through [Step 5](#) until you have added all of the new license files.
- Step 7** On the Licenses page, check the check boxes for the license files that you added in [Step 2](#) through [Step 5](#).
- Step 8** Click **Install Selected**.
- Step 9** If Connection is not configured for a cluster, skip the remaining steps.
- If you are adding licensed features to a Connection cluster that is already installed and in use, skip the remaining steps.
- If you are installing a new Connection cluster, on the subscriber server, in Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 10** On the Search License page, click **Add New**.
- Step 11** On the Add New License page, click **Browse**, and locate the new license file.
- Step 12** In the Choose File dialog box, double-click the name of the license file that has the MAC address of the subscriber server.

**Caution**

If you rename the license file, the file name can contain alphanumeric characters, hyphens, and underscores, but must start with an alphabetic character. Otherwise, the license file cannot be installed.

- Step 13** On the Add New License page, click **Add**.
- Step 14** If you have more than one new license file, repeat [Step 10](#) through [Step 13](#) until you have added all of the new license files.
- Step 15** On the Licenses page, check the check boxes for the license files that you added in [Step 10](#) through [Step 13](#).
- Step 16** Click **Install Selected**.

Viewing Reports for Licenses

Added May 2009

Cisco Unity Connection can display the following information about Connection licenses:

- **License Usage**—Shows the status of licensed features for the Connection server. For features that are licensed for a number of seats, the report displays the number of used and unused seats. See the [“Viewing the License Usage” section on page 44-5](#).

- **License Expirations**—Shows the expiration dates, if any, for licensed features for the Connection server. A list of installed and uninstalled license files also appears on the report. See the [“Viewing the License Expirations”](#) section on page 44-5.

Viewing the License Usage

Do the applicable procedure to view the license usage for the Cisco Unity Connection server.

To View the License Usage for Cisco Unity Connection 7.1 and Later

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 2** On the Licenses page, under License Count, the license usage for the Connection server appears.
-

To View the License Usage for Cisco Unity Connection 7.0 Only

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 2** On the Licenses page, in the Related links list, click **View License Usage**.
- Step 3** Click **Go**.
- The Cisco Unity Connection Administration Task Alerts window shows the License Usage for the Connection server.
-

Viewing the License Expirations

Do the applicable procedure to view the license expirations for the Cisco Unity Connection server.

To View the License Expirations for Cisco Unity Connection 7.1 and Later

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 2** On the Licenses page, in the Status area, license expirations for the Connection server appear.
-

To View the License Expirations for Cisco Unity Connection 7.0 Only

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 2** On the Licenses page, in the Related links list, click **Run License Report**.
- Step 3** Click **Go**.
- The Cisco Unity Connection Administration Task Alerts window shows the License Report for the Connection server.
-

License Parameters for Cisco Unity Connection Features

Added May 2009

Table 44-1 lists the license parameters that are used by license files and the Cisco Unity Connection features that the license parameters enable.

Table 44-1 License Parameters for Cisco Unity Connection Features

License Parameter	Feature	Description
LicAdvancedUserMax	TTS and ASR (advanced) users	Sets the maximum number of users who can use voice recognition.
LicIMAPSubscribersMax	Users with IMAP access to voice messages	Sets the maximum number of users who can use a third-party IMAP client to access voice messages.
LicMaxMsgRecLenIsLicensed	Voice message recordings longer than 30 seconds allowed	<p>Depending on whether the parameter is present in any of the installed license files, determines the maximum length of recorded messages:</p> <ul style="list-style-type: none"> If the parameter is not present in any of the installed license files (the License Usage report shows a value of “No”), the maximum message length is 30 seconds regardless of the settings in Cisco Unity Connection Administration. If the parameter is present in any of the installed license files (the License Usage report shows a value of “Yes”), the maximum length for all messages is restricted by the Maximum Recording Time in Milliseconds field on the System Settings > Advanced > Telephony > Telephony Configuration page. <p>The following settings further restrict the maximum length depending on the origin of the call:</p> <ul style="list-style-type: none"> Message length from other users is restricted by the Message Length—Maximum Length field on the Class of Service > Class of Service > Edit Class of Service page. Message length from unidentified callers is restricted by the Maximum Message Length field on the Users > Users > Edit Message Settings page.
LicRealspeakSessionsMax	Text to Speech sessions	Sets the maximum number of simultaneous Text to Speech (TTS) sessions allowed on the Cisco Unity Connection server.

Table 44-1 License Parameters for Cisco Unity Connection Features (continued)

License Parameter	Feature	Description
LicRegionIsUnrestricted	U.S. English usage and personal call routing rules allowed	Depending on whether the parameter is present in any of the installed license files, determines whether the English-United States language and personal call transfer rules are allowed: <ul style="list-style-type: none"> If the parameter is not present in any of the installed license files (the License Usage report shows a value of “No”), the English-United States language and personal call transfer rules are not allowed. If the parameter is present in any of the installed license files (the License Usage report shows a value of “Yes”), the English-United States language and personal call transfer rules are allowed.
LicServerBackend	(not used)	This parameter may be present in a license file but does not affect the Cisco Unity Connection server.
LicServerVoiceRec	(not used)	This parameter may be present in a license file but does not affect the Cisco Unity Connection server.
LicSubscribersMax	Users with voice mailboxes	Sets the maximum number of voice messaging users allowed in Cisco Unity Connection.
LicUCxnUpgrades	License files from previous releases allowed	Depending on whether the parameter is present in any of the installed license files, determines whether Cisco Unity Connection will use license files from an earlier version of Connection: <ul style="list-style-type: none"> If the parameter is not present in any of the installed license files (the License Usage report shows a value of “No”), license files from an earlier version of Connection cannot be used. If the parameter is present in any of the installed license files (the License Usage report shows a value of “Yes”), license files from an earlier version of Connection can be used.
LicUnityVoiceRecSessionsMax	Voice recognition sessions	Sets the maximum number of simultaneous voice recognition sessions (or ports) allowed on the Cisco Unity Connection server.
LicVMISubscribersMax	Cisco Unity Inbox users	Sets the maximum number of users who can be enabled to access the Cisco Unity Inbox. There is no restriction on the number of users who can access the Cisco Unity Inbox at one time.
LicVoicePortsMax	Voice ports	Sets the maximum number of Cisco Unity Connection voice messaging ports that can be installed on the Connection server.

Table 44-1 *License Parameters for Cisco Unity Connection Features (continued)*

License Parameter	Feature	Description
LicVPIMIsLicensed	VPIM Networking delivery locations allowed	<p>Depending on whether the parameter is present in any of the installed license files, determines whether VPIM Networking is allowed:</p> <ul style="list-style-type: none"> • If the parameter is not present in any of the installed license files (the License Usage report shows a value of “No”), VPIM Networking is not allowed. • If the parameter is present in any of the installed license files (the License Usage report shows a value of “Yes”), VPIM Networking is allowed.



INDEX

A

- abbreviated extensions [6-10](#)
- accounts
 - Operator [19-6](#)
 - UndeliverableMessagesMailbox [19-6](#)
 - Unity Connection Messaging System [19-6](#)
- adding
 - alternate names for a system distribution list [27-4](#)
 - AXL servers [29-5](#)
 - Cisco Unified Communications Manager servers [29-10](#)
 - description of message attachments [39-1](#)
 - global nicknames to list [14-12](#)
 - integration, phone system [29-2](#)
 - members to system distribution lists [27-3](#)
 - PIMG/TIMG units [29-15](#)
 - port [29-17](#)
 - port group [29-8](#)
 - SIP server [29-13](#)
 - system distribution lists [27-2](#)
 - TFTP server [29-12](#)
- addressing options, VPIM Networking [34-17](#)
- AGC, changing settings for port group [29-17](#)
- All Hours schedule [10-1](#)
- All Voice Mail Users distribution list [27-1](#)
- alternate contact numbers, configuring for call handlers [6-8](#)
- alternate conversations
 - Optional Conversation 1 [13-3](#)
 - overview [13-3](#)
- alternate names
 - adding for system distribution lists [27-4](#)
 - adding for VPIM locations [34-13](#)
- application plug-ins [3-1](#)
- Attempt Forward call routing rule [9-1](#)
- Attempt Sign-In call routing rule [9-1](#)
- audio format
 - changing for calls [16-1, 29-9](#)
 - changing for recordings [16-2, 17-5, 19-4](#)
 - VPIM Networking [34-18](#)
- authentication, configuring LDAP [43-5](#)
- authentication rules
 - default rules [18-2](#)
 - overview [18-2](#)
- automated attendant [4-9](#)
- automatic gain control (AGC), changing settings for port group [29-17](#)
- AXL servers
 - adding [29-5](#)
 - changing settings [29-7](#)
 - deleting [29-7](#)

B

- backing up and restoring data [3-7](#)
- backup and restore application for migrations (COBRAS) [3-2](#)
- blind addressing, VPIM Networking [34-17](#)
- Broadcast Message Administrator
 - setting up access [26-2](#)
 - using [26-5](#)
- broadcast messages
 - changing default settings [26-6](#)
 - overview [26-1](#)
 - setting up access for sending [26-2](#)
- Bulk Administration Tool
 - accessing [3-2](#)

creating VPIM contacts [34-7, 34-8](#)

errors, correcting (VPIM) [34-8](#)

Bulk Edit utility, accessing [3-3](#)

C

calendar integration

about [35-1](#)

changing user configurations for the Cisco Unified MeetingPlace Express integration [35-32](#)

changing user configurations for the Cisco Unified MeetingPlace integration [35-24](#)

changing user configurations for the Exchange 2003 integration [35-17](#)

changing user configurations for the Exchange 2007 integration [35-8](#)

changing with Cisco Unified MeetingPlace [35-23](#)

changing with Cisco Unified MeetingPlace Express [35-30](#)

changing with Exchange 2003 [35-16](#)

changing with Exchange 2007 [35-8](#)

creating with Cisco Unified MeetingPlace [35-18](#)

creating with Cisco Unified MeetingPlace Express [35-25](#)

creating with Exchange 2003 [35-10](#)

creating with Exchange 2007 [35-1](#)

Exchange contacts [35-1](#)

caller input settings, changing user logon settings [14-7](#)

caller options, user settings [13-5](#)

call handlers

caller input and one-key dialing [6-8](#)

call transfer settings [6-12](#)

default [6-1](#)

deleting [6-12](#)

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 [4-5](#)

taking messages [6-11](#)

templates, modifying [6-3](#)

call handler templates

creating [6-2](#)

default templates [6-2](#)

deleting [6-2](#)

modifying [6-2](#)

Call Handler Traffic report [41-3](#)

call holding, user settings in Cisco Unity Assistant [13-5](#)

call loop detection [29-4](#)

call management

creating a map [5-1](#)

implementing a plan [5-2](#)

managing call handlers [6-1](#)

managing call routing tables [9-1](#)

managing directory handlers [7-1](#)

managing interview handlers [8-1](#)

managing restriction tables [11-1](#)

managing schedules and holidays [10-1](#)

overview [4-1](#)

planning [5-1](#)

call routing tables

adding rules [9-2](#)

and the Route From Next Call Routing Rule action [4-5](#)

Attempt Forward rule [9-1](#)

Attempt Sign-In rule [9-1](#)

changing the order of rules [9-3](#)

default rules [9-1](#)

deleting rules [9-3](#)

modifying rules [9-2](#)

Opening Greeting rule [9-1](#)

overview [4-3](#)

calls, changing the audio format (or codec) for [16-1, 29-9](#)

call screening, user settings in Cisco Unity Assistant [13-5](#)

call transfers

user settings in Cisco Unity Assistant [13-5](#)

- user settings in Connection conversation [13-5](#)
- call waiting, configuring hold time [14-3](#)
- capacity of hard disk, specifying maximum percentage [19-17](#)
- certificate, viewing for port [29-20](#)
- changing
 - addressing and recording order [14-1, 14-3](#)
 - addressing priority lists, how names are stored in [14-2](#)
 - AGC settings [29-17](#)
 - AXL server settings [29-7](#)
 - call loop detection settings [29-4](#)
 - Cisco Unified Communications Manager server settings [29-11](#)
 - codec preference settings [29-9](#)
 - description of message attachments [39-2](#)
 - dial prefix settings for live reply to unidentified callers [14-5](#)
 - message deletion options [14-5](#)
 - message skipping during playback (Optional Conversation 1) [14-10](#)
 - MWI settings [29-10](#)
 - phone system settings [29-3](#)
 - phone system trunk settings [29-21](#)
 - PIMG/TIMG settings [29-16](#)
 - port group advanced settings [29-16](#)
 - port group settings [29-9](#)
 - port settings [29-18](#)
 - SIP server settings [29-14](#)
 - SIP settings [29-16](#)
 - system prompt language [14-6](#)
 - TFTP server settings [29-13](#)
 - user logon settings during user greeting [14-7](#)
- Cisco DirSync service, activating [43-3](#)
- Cisco Fax Server integration
 - about [32-1](#)
 - changing the Cisco Unity Connection configuration [32-8](#)
 - changing the user configuration [32-9](#)
 - configuring Cisco Unity Connection [32-5](#)
 - configuring single number for calls and faxes [32-9](#)
 - configuring the Cisco Fax Server [32-2](#)
 - configuring users [32-7](#)
 - creating [32-1](#)
 - requirements [32-2](#)
 - testing [32-7](#)
- Cisco PCA, securing access to Cisco Unity Connection [25-1](#)
- Cisco SIP Proxy Server
 - adding [29-13](#)
 - changing settings [29-14](#)
 - deleting [29-14](#)
- Cisco Unified Communications Manager
 - adding servers [29-10](#)
 - adding TFTP server [29-12](#)
 - AXL servers, adding [29-5](#)
 - AXL servers, deleting [29-7](#)
 - changing AXL server settings [29-7](#)
 - changing server settings [29-11](#)
 - changing TFTP server settings [29-13](#)
 - deleting servers [29-11](#)
 - deleting TFTP server [29-12](#)
 - port certificate [29-20](#)
 - root certificate for Connection [29-22](#)
- Cisco Unified MeetingPlace
 - changing the calendar integration [35-23](#)
 - changing user configurations for the calendar integration [35-24](#)
 - creating a calendar integration [35-18](#)
- Cisco Unified MeetingPlace Express
 - changing the calendar integration [35-30](#)
 - changing user configurations for the calendar integration [35-32](#)
 - creating a calendar integration [35-25](#)
- Cisco Unified Mobility Advantage integration
 - about [30-1](#)
 - configuring Cisco Unity Connection [30-2](#)
 - requirements [30-2](#)
 - task list for creating [30-1](#)
 - testing [30-3](#)

Cisco Unified Real-Time Monitoring Tool (RTMT) [3-7](#)

Cisco Unified Serviceability [3-8](#)

Cisco Unified Serviceability services

 configuring enterprise parameters [37-1](#)

 configuring service parameters [36-1](#)

 descriptions of enterprise parameters [37-2](#)

 descriptions of service parameters [36-2](#)

Cisco Unity Connection Administration

 accessing [2-1](#)

 configuring browsers [1-1](#)

 finding records [2-3](#)

 interface [2-2](#)

 using Help [2-2](#)

Cisco Unity Connection conversation [13-1](#)

Cisco Unity Greetings Administrator

 overview [17-2](#)

 setting up [17-4](#)

 using [17-3](#)

Cisco Utilities Database Link for Informix [3-10](#)

Cisco Voice Technology Group Subscription tool [3-7](#)

cluster, configuring and customizing [42-1](#)

COBRAS backup and restore application [3-2](#)

codec

 changing for calls [16-1, 29-9](#)

 changing for recordings [16-2, 17-5, 19-4](#)

 changing preference settings [29-9](#)

configuring

 access to emails in external message store [40-1](#)

 call waiting hold time [14-3](#)

 cross-server logon and transfers [33-13](#)

 one-key dialing [6-8](#)

 smart host, for Digital Networking [33-10](#)

Connection 1.x, migrating from [3-2](#)

Connection Administration, accessing [3-2](#)

Connection locations

 manually synchronizing [33-17](#)

 overview [33-19](#)

 removing from the Digital Network [33-18](#)

Connection Serviceability [3-6](#)

Connection User Data Dump [3-10](#)

conversation

 allowing voice recognition users to say their voice
 mail passwords [14-10](#)

 alternate conversation versions [13-3](#)

 caller options [13-1](#)

 changing addressing and recording order [14-1, 14-3](#)

 changing dial prefix settings for live reply to
 unidentified callers [14-5](#)

 changing how names are stored in user addressing
 priority lists [14-2](#)

 changing message deletion options [14-5](#)

 changing password re-entry behavior [14-8](#)

 Cisco Unity Connection, overview [13-1](#)

 customizing by administrators [13-2](#)

 customizing by users [13-5](#)

 documenting for users [3-10](#)

 easy sign-in [14-8](#)

 sign-in [14-8](#)

 specifying caller information before message
 playback [14-4](#)

 user options [13-1](#)

 user settings in Cisco Unity Assistant [13-6](#)

 user settings in Connection conversation [13-6](#)

 using voice commands [13-3](#)

creating

 AXL servers [29-5](#)

 call handler templates [6-2](#)

 call management map [5-1](#)

 call routing rules [9-2](#)

 directory handlers [7-1](#)

 holiday schedules [10-1](#)

 interview handlers [8-1](#)

 restriction tables [11-1](#)

 schedules [10-2](#)

 user accounts [ii-xix](#)

credentials policies [18-1](#)

cross-server logon and transfers

 configuring [33-13](#)

 overview [33-23](#)

CSV files

- correcting errors for Bulk Administration Tool [34-8](#)
- creating VPIM contacts [34-7](#)

CUDLI [3-10](#)

Custom Keypad Mapping tool

- accessing [15-1](#)
- conversations that can be customized [15-3](#)
- documenting keypad for users [15-13](#)
- guidelines [15-2](#)
- resetting [15-2](#)
- using [15-1](#)

D

Database Proxy [3-8](#)

deleting

- AXL servers [29-7](#)
- call handlers [6-12, 7-4](#)
- call handler templates [6-2](#)
- call routing rules [9-3](#)
- Cisco Unified Communications Manager servers [29-11](#)
- description of message attachments [39-2](#)
- integration, phone system [29-2](#)
- interview handlers [8-3](#)
- members from system distribution lists [27-3](#)
- phone system trunk [29-21](#)
- PIMG/TIMG units [29-15](#)
- port [29-18](#)
- port group [29-9](#)
- restriction tables [11-3](#)
- schedules [10-3](#)
- SIP server [29-14](#)
- TFTP server [29-12](#)

delivery locations, creating for VPIM [34-6](#)

demonstration license files, about [44-2](#)

Dial Plan report [41-4](#)

Dial Search Scope report [41-4](#)

Digital Networking

adding a server to an existing network [33-8](#)

addressing options for non-networked phone systems [33-21](#)

and Connection locations [33-19](#)

and object replication [33-20](#)

and private distribution lists [33-24](#)

and system distribution lists [33-23](#)

and VPIM locations [33-24](#)

broadcast messages not supported between locations [33-25](#)

checking or modifying the server display name and SMTP domain name [33-5](#)

checking replication status [33-9](#)

cleaning up unused VPIM locations and contacts [33-17](#)

client access to servers [33-25](#)

configuring a smart host [33-10](#)

configuring cross-server logon and transfers [33-13](#)

configuring search spaces for [33-12](#)

configuring SMTP access for cluster subscriber servers [33-11](#)

creating a network-wide all voice mail users distribution list [33-16](#)

cross-server logon and transfer overview [33-23](#)

deployment decisions [33-4](#)

identified user messaging between networked users [33-22](#)

joining two servers to create a Digital Network [33-6](#)

manually synchronizing locations [33-17](#)

mapping users to systems [33-25](#)

notable behavior [33-24](#)

overview [33-1](#)

prerequisites [33-2](#)

removing a location from the network [33-18](#)

replication suspended during bulk operations [33-25](#)

replication with clusters [33-25](#)

securing [33-13](#)

setting up [33-2](#)

setup task list [33-2](#)

testing the setup [33-14](#)

directory handlers

- creating [7-1](#)
- default [7-1](#)
- deleting [7-4](#)
- modifying [7-2](#)
- overview [4-2](#)
- System Directory Handler [7-1](#)

Disaster Recovery System [3-7](#)

dispatch messages [19-6](#)

Distribution Lists report [41-2](#)

DNS, resolving names with IP addresses [34-4](#)

E

easy sign-in conversation [14-8](#)

Edit Disk Capacity Configuration page [19-17](#)

email

- configuring access in external message store [40-1](#)
- messages [19-2](#)

end of recording, configuring termination warning prompt [19-5](#)

enterprise parameters

- configuring for Cisco Unified Serviceability services [37-1](#)
- descriptions [37-2](#)
- for Cisco Unified Serviceability services [37-1](#)

Exchange 2003

- changing the calendar integration [35-16](#)
- changing user configurations for the calendar integration [35-17](#)
- creating a calendar integration [35-10](#)

Exchange 2007

- changing the calendar integration [35-8](#)
- changing user configurations for the calendar integration [35-8](#)
- creating a calendar integration [35-1](#)

Exchange contacts

- enabling importing from Exchange 2003 [35-10](#)
- enabling importing from Exchange 2007 [35-1](#)

extensions

- adding prepended digits [6-10](#)

- converting LDAP phone numbers into [43-4](#)

external message store, configuring access to emails in [40-1](#)

F

fax

- about the Cisco Fax Server integration [32-1](#)
- changing the Cisco Unity Connection configuration [32-8](#)
- changing the user configuration [32-9](#)
- configuring Cisco Unity Connection [32-5](#)
- configuring single number for calls and faxes [32-9](#)
- configuring the Cisco Fax Server [32-2](#)
- configuring users [32-7](#)
- creating a Cisco Fax Server integration [32-1](#)
- requirements for the Cisco Fax Server integration [32-2](#)
- testing [32-7](#)

field definitions [2-2](#)

Firefox, configuring [1-1](#)

G

G.711 A-Law codec

- selecting for calls [16-1, 29-9](#)
- selecting for recordings [16-2, 17-5, 19-4](#)

G.711 Mu-Law codec

- selecting for calls [16-1, 29-9](#)
- selecting for recordings [16-2, 17-5, 19-4](#)

G.729a codec

- selecting for calls [16-1, 29-9](#)
- selecting for recordings [16-2, 17-5, 19-4](#)

G726 codec, selecting for recordings [16-2, 17-5, 19-4](#)

global nicknames

- adding names to list [14-12](#)
- editing list [14-12](#)

Goodbye call handler [6-2](#)

Grammar Statistics tool, accessing [3-4](#)

greetings

- call handlers [6-6](#)
- changing audio format for recording [17-5](#)
- recording by using Media Master [17-1](#)
- user settings in Cisco Unity Assistant [13-6](#)
- user settings in Connection conversation [13-6](#)

groupware email messages [19-2](#)

H

hard disk, specifying maximum capacity [19-17](#)

Help

- page and field [2-2](#)
- using [2-2](#)

holidays

- designating [10-1](#)
- holiday schedule [10-1](#)

I

identified user messaging

- and Digital Networking [33-22](#)
- overview [19-2](#)

IMAP access

- accessing email messages from Connection by using [19-2](#)
- configuration procedures [20-4](#)
- configuration task list [20-3](#)
- Connection server configuration [20-5](#)
- security recommendations [20-3](#)
- SMTP message parameters [20-7](#)

IMAP clients

- integrated messaging example [20-2](#)
- securing access to Cisco Unity Connection [25-1](#)
- security options [24-3](#)
- SMTP message handling [20-1](#)

Import Users tool, accessing [3-4](#)

installing license files [44-2](#)

integrated messaging, example [20-2](#)

integration

- adding [29-2](#)
- adding phone system trunk [29-21](#)
- adding PIMG/TIMG units [29-15](#)
- adding port [29-17](#)
- adding port group [29-8](#)
- adding SIP certificate [29-24](#)
- adding SIP security profile [29-25](#)
- adding SIP server [29-13](#)
- adding TFTP server [29-12](#)
- AXL server, changing settings [29-7](#)
- AXL servers, adding [29-5](#)
- AXL servers, deleting [29-7](#)
- call loop detection, changing settings [29-4](#)
- changing AGC settings [29-17](#)
- changing Cisco Unified Communications Manager server settings [29-11](#)
- changing phone system trunk settings [29-21](#)
- changing PIMG/TIMG settings [29-16](#)
- changing port group advanced settings [29-16](#)
- changing port settings [29-18](#)
- changing SIP certificate [29-24](#), [29-25](#)
- changing SIP server settings [29-14](#)
- changing SIP settings [29-16](#)
- changing TFTP server settings [29-13](#)
- codec, changing preference settings [29-9](#)
- deleting [29-2](#)
- deleting Cisco Unified Communications Manager servers [29-11](#)
- deleting phone system trunk [29-21](#)
- deleting PIMG/TIMG units [29-15](#)
- deleting port [29-18](#)
- deleting SIP certificate [29-24](#)
- deleting SIP security profile [29-25](#)
- deleting SIP server [29-14](#)
- deleting TFTP server [29-12](#)
- MWI, disabling the use of the same port for turning on and off [29-3](#)
- MWI, synchronizing [29-4](#)
- MWIs, changing settings [29-10](#)

- phone system, changing settings [29-3](#)
- phone system trunk description [29-20](#)
- port certificate [29-20](#)
- port description [29-17](#)
- port group, changing settings [29-9](#)
- port group, deleting [29-9](#)
- port group description [29-7](#)
- root certificate for Connection [29-23](#)
- security for ports [29-22](#)
- users associated with phone system [29-3](#)
- viewing root certificate for Connection [29-22](#)

Internet Explorer, configuring [1-2](#)

interview handlers

- creating [8-1](#)
- deleting [8-3](#)
- modifying [8-2](#)
- overview [4-3](#)

L

language

- changing system prompt language [14-6](#)
- language settings for call handlers [6-11](#)
- language settings for directory handlers [7-3](#)
- language settings for interview handlers [8-2](#)
- language settings for routing rules [9-3](#)
- message subject line format [19-13](#)

LDAP

- activating the Cisco DirSync service [43-3](#)
- adding configurations and synchronizing data [43-7](#)
- configuring authentication [43-5](#)
- converting LDAP phone numbers into Connection extensions [43-4](#)
- enabling synchronization [43-3](#)
- task list for configuring [43-2](#)

license files

- about using MAC addresses [44-1](#)
- about using multiple license files [44-2](#)
- Connection clusters [44-2](#)

- must be installed [44-2](#)

- obtaining and installing [44-2](#)

- parameters for Connection features [44-6](#)

- permanent, time-expiring, and demonstration [44-2](#)

- viewing reports [44-4](#)

live record

- about [19-4](#)

- configuring [19-18](#)

lockout policy [18-1](#)

logon policy [18-1](#)

M

mailboxes, moving [21-4](#)

mailbox size quotas, setting systemwide and mailbox-store limits [22-1](#)

Mailbox Store report [41-4](#)

mailbox stores

- backing up [21-3](#)

- creating [21-4](#)

- deleting [21-5](#)

- disabling [21-7](#)

- maximum size [21-2](#)

- maximum size, changing [21-5](#)

- message handling when maximum size is exceeded [19-11](#)

- moving mailboxes [21-4](#)

- multiple [21-1](#)

Maximum Delay for TTS Access Before Timeout [19-9](#)

Media Master

- preventing users from saving messages [24-3](#)

- recording greetings and names [17-1](#)

MeetingPlace

- changing the calendar integration [35-23](#)

- changing user configurations for the calendar integration [35-24](#)

- creating a calendar integration [35-18](#)

MeetingPlace Express

- changing the calendar integration [35-30](#)

- changing user configurations for the calendar integration [35-32](#)
 - creating a calendar integration [35-25](#)
- message actions, configuring [19-13](#)
- message addressing
 - user settings in Cisco Unity Assistant [13-7](#)
 - user settings in Connection conversation [13-7](#)
- message attachment
 - adding [39-1](#)
 - changing [39-2](#)
 - deleting [39-2](#)
- message locator, phone view [31-1](#)
- message notification
 - setting up, SMS (SMPP) [23-2](#)
 - setting up, SMTP [23-1](#)
 - user settings in Cisco Unity Assistant [13-6](#)
 - user settings in Connection conversation [13-6](#)
- message playback
 - user settings in Cisco Unity Assistant [13-7](#)
 - user settings in Connection conversation [13-7](#)
- messages
 - actions, configuring [19-13](#)
 - dispatch messages [19-6](#)
 - groupware email messages [19-2](#)
 - how Connection handles messages that are interrupted by disconnected calls [19-10](#)
 - how Connection handles messages that cannot be delivered [19-9](#)
 - how Connection handles messages when mailbox quotas are exceeded [19-11](#)
 - how Connection handles messages when maximum mailbox store size is exceeded [19-11](#)
 - how Connection handles messages when system components are unavailable [19-9](#)
 - interview messages [19-3](#)
 - live record [19-4](#)
 - message delivery [19-9](#)
 - message storage [19-17](#)
 - 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 [19-3](#)
 - outside caller voice messages [19-1](#)
 - receipts [19-3](#)
 - security options for IMAP client access [24-3](#)
 - sensitivity [19-12](#)
 - subject line format [19-13](#)
 - system broadcast messages [19-2](#)
 - types of messages [19-1](#)
 - user to user voice messages [19-2](#)
 - VPIM [34-16](#)
- message security
 - call handlers [6-11](#)
 - option to disable saves in Media Master [24-3](#)
 - overview of options [24-1](#)
 - sensitivity options for users and unidentified callers [24-1](#)
- Message Traffic report [41-2](#)
- message waiting indicators, synchronizing for phone system [29-4](#)
- messaging overview [19-1](#)
- 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](#)
 - call routing rules [9-2](#)
 - directory handlers [7-2](#)
 - interview handlers [8-2](#)
 - restriction tables [11-3](#)
 - schedules [10-2](#)
 - system distribution lists [27-3, 27-4](#)
- multiple mailbox stores [21-1](#)
- MWIs
 - changing settings [29-10](#)

disabling the use of the same port for turning on and off [29-3](#)
 synchronizing for phone system [29-4](#)

N

name resolution, VPIM [34-4](#)
 names, recording by using Media Master [17-1](#)
 notification
 setting up, SMS (SMPP) [23-2](#)
 setting up, SMTP [23-1](#)
 user settings in Cisco Unity Assistant [13-6](#)
 user settings in Connection conversation [13-6](#)

O

obtaining license files [44-2](#)
 one-key dialing
 configuring [6-8](#)
 overview [6-8](#)
 Opening Greeting
 call handler [6-1](#)
 call routing rule [9-1](#)
 Operator call handler [6-2](#)
 Operator user [19-6](#)
 Optional Conversation 1
 changing message skipping behavior [14-10](#)
 overview [13-3](#)
 Outcall Billing Detail report [41-3](#)
 Outcall Billing Summary report [41-3](#)
 outside caller voice messages [19-1](#)

P

page Help [2-2](#)
 partitions
 changing default [28-11](#)
 creating [28-8](#)
 default [28-2](#)

deleting [28-9](#)
 finding objects in [28-11](#)
 modifying [28-9](#)
 overview [28-1](#)
 password policy [18-1](#)
 PCM codec, selecting for recordings [16-2, 17-5](#)
 permanent license files, about [44-2](#)
 personal contacts, user settings in Cisco Unity Assistant [13-8](#)
 personal settings
 user settings in Cisco Unity Assistant [13-7](#)
 user settings in Connection conversation [13-7](#)
 Phone Interface Failed Logon report [41-1](#)
 phone language, changing [14-6](#)
 phone system
 adding AXL servers [29-5](#)
 adding integration [29-2](#)
 changing AXL server settings [29-7](#)
 changing settings [29-3](#)
 deleting AXL servers [29-7](#)
 deleting integration [29-2](#)
 disabling the use of the same port for turning on and off an MWI [29-3](#)
 list of users associated with [29-3](#)
 synchronizing MWIs [29-4](#)
 phone system trunk
 changing settings [29-21](#)
 deleting [29-21](#)
 description [29-20](#)
 Phone View [29-4, 31-1](#)
 PIMG unit
 adding [29-15](#)
 changing settings [29-16](#)
 deleting [29-15](#)
 PIN policy [18-1](#)
 plugins
 application [3-1](#)
 installing [38-1](#)
 overview [38-1](#)

Port Activity report [41-2](#)

port group

- adding [29-8](#)
- changing advanced settings [29-16](#)
- changing AGC settings [29-17](#)
- changing settings [29-9](#)
- deleting [29-9](#)
- description [29-7](#)

port memory, disabling [29-3](#)

ports

- adding [29-17](#)
- adding SIP certificate [29-24](#)
- adding SIP security profile [29-25](#)
- changing settings [29-18](#)
- changing SIP certificate [29-24, 29-25](#)
- deleting [29-18](#)
- deleting SIP certificate [29-24](#)
- deleting SIP security profile [29-25](#)
- description [29-17](#)
- port certificate for Connection [29-20](#)
- root certificate for Connection [29-23](#)
- security [29-22](#)
- viewing root certificate for Connection [29-22](#)

prepended digits for extensions [6-10](#)

prerequisites

- Digital Networking [33-2](#)
- VPIM Networking [34-2](#)

private lists

- and Digital Networking [33-24](#)
- user settings in Cisco Unity Assistant [13-7](#)
- user settings in Connection conversation [13-7](#)

prompts

- overview [13-2](#)
- what you can change [13-2](#)

Q

quotas, message handling when exceeded [19-11](#)

R

recordings

- changing the audio format (or codec) for [16-2, 17-5, 19-4](#)
- configuring termination warning prompt [19-5](#)
- greetings and names [17-1](#)
- selecting device [17-2](#)

relay settings for private and secure messages [20-5](#)

Remote Administration Tools [3-8](#)

replication

- Digital Networking, checking status of [33-9](#)
- overview [33-20](#)
- suspended during bulk operations [33-25](#)
- with clusters [33-25](#)

reports

- archiving data [41-5](#)
- Call Handler Traffic [41-3](#)
- configuration parameters [41-4](#)
- Dial Plan [41-4](#)
- Dial Search Scope [41-4](#)
- Distribution Lists [41-2](#)
- generating and viewing [41-5](#)
- licenses [44-4](#)
- Mailbox Store [41-4](#)
- Message Traffic [41-2](#)
- Outcall Billing Detail [41-3](#)
- Outcall Billing Summary [41-3](#)
- overview [41-1](#)
- Phone Interface Failed Logon [41-1](#)
- Port Activity [41-2](#)
- Subscriber Message Activity [41-2](#)
- System Configuration [41-3](#)
- Transfer Call Billing [41-3](#)
- Unused Voice Mail Accounts [41-3](#)
- User Lockout [41-3](#)
- Users [41-1](#)

restriction tables

- creating [11-1](#)

- default [11-1](#)
- Default Fax [11-1](#)
- Default Outdial [11-1](#)
- Default System Transfer [11-1](#)
- Default Transfer [11-1](#)
- deleting [11-3](#)
- modifying [11-3](#)
- overview [4-6](#)
- root certificate
 - saving as file [29-23](#)
 - viewing [29-22](#)
- Route From Next Call Routing Rule action [4-5](#)
- RSS Feeds [19-20](#)

S

- schedules and holidays
 - All Hours [10-1](#)
 - creating schedules [10-2](#)
 - default [10-1](#)
 - deleting schedules [10-3](#)
 - designating holidays [10-1](#)
 - Holidays [10-1](#)
 - modifying schedules [10-2](#)
 - overview [4-8](#)
 - Voice Recognition Update [10-1](#)
 - Weekdays [10-1](#)
- search spaces
 - and call handlers [28-7](#)
 - and call routing rules [28-6](#)
 - and digital networking [28-7](#)
 - and directory handlers [28-7](#)
 - and interview handlers [28-7](#)
 - and system contacts [28-8](#)
 - and system distribution lists [28-6](#)
 - and user objects [28-5](#)
 - and VPIM locations [28-8](#)
 - changing default [28-11](#)
 - configuring for Digital Networking [33-12](#)

- creating [28-10](#)
- default [28-2](#)
- deleting [28-10](#)
- example configurations [28-3](#)
- finding objects in [28-11](#)
- modifying [28-10](#)
- overview [28-2](#)
- securing Cisco PCA and IMAP client access to Cisco Unity Connection [25-1](#)
- security
 - adding SIP certificate [29-24](#)
 - adding SIP security profile [29-25](#)
 - changing SIP certificate [29-24, 29-25](#)
 - controlling access, distribution, and storage of voice messages [24-1](#)
 - deleting SIP certificate [29-24](#)
 - deleting SIP security profile [29-25](#)
 - description for ports [29-22](#)
 - IMAP client [24-3](#)
 - policies [18-1](#)
 - port certificate [29-20](#)
 - relay settings for private and secure messages [20-5](#)
 - root certificate for Connection [29-23](#)
 - user and unidentified caller messages [24-1](#)
 - viewing root certificate for Connection [29-22](#)
- service parameters
 - configuring for Cisco Unified Serviceability services [36-1](#)
 - descriptions [36-2](#)
 - for Cisco Unified Serviceability services [36-1](#)
- Session Initiation Protocol (SIP), changing settings [29-16](#)
- session timeout setting, Cisco Unity Connection Administration [2-1](#)
- setting up
 - SMS (SMPP) message notifications [23-2](#)
 - SMTP message notifications [23-1](#)
- sign-in conversation [14-8](#)
- simulating abbreviated extensions [6-10](#)
- SIP
 - adding SIP certificate [29-24](#)

- adding SIP security profile [29-25](#)
- changing SIP certificate [29-24, 29-25](#)
- deleting SIP certificate [29-24](#)
- deleting SIP security profile [29-25](#)
- SIP server
 - adding [29-13](#)
 - changing settings [29-14](#)
 - deleting [29-14](#)
- smart host, configuring for Digital Networking [33-10](#)
- SMS (SMPP) message notifications, setting up [23-2](#)
- SMTP
 - message notifications, setting up [23-1](#)
 - messages, overview [20-1](#)
- SSL certificate, using to secure Cisco PCA and IMAP client access to Cisco Unity Connection [25-1](#)
- Subscriber Information Dump. See Connection User Data Dump.
- Subscriber Message Activity report [41-2](#)
- synchronizing MWIs for phone system [29-4](#)
- Synch Users Tool, accessing [3-4](#)
- System Configuration report [41-3](#)
- System Directory Handler [7-1](#)
- system distribution lists
 - adding alternate names [27-4](#)
 - adding and removing members [27-3](#)
 - and Digital Networking [33-23](#)
 - creating [27-2](#)
 - default lists [27-1](#)
 - modifying [27-3, 27-4](#)
 - overview [27-1](#)
- system prompts
 - changing language [14-6](#)
 - customizing [13-2](#)
- system transfers, setting up [12-1](#)

T

- Task Management tool, accessing [3-7](#)
- termination warning prompt, configuring [19-5](#)

- TFTP server
 - adding [29-12](#)
 - changing settings [29-13](#)
 - deleting [29-12](#)
- time-expiring license files, about [44-2](#)
- timeouts in Cisco Unity Connection Administration [2-1](#)
- TIMG unit
 - adding [29-15](#)
 - changing settings [29-16](#)
 - deleting [29-15](#)
- tools, Custom Keypad Mapping [15-1](#)
- Transfer Call Billing report [41-3](#)
- trunk, phone system
 - adding [29-21](#)
 - changing settings [29-21](#)
 - deleting [29-21](#)

U

- Undeliverable Messages distribution list [27-2](#)
- UndeliverableMessagesMailbox user [19-6](#)
- unidentified caller messages [19-1](#)
- Unity, migrating from [3-2](#)
- Unity Connection Messaging System user [19-6](#)
- Unused Voice Mail Accounts report [41-3](#)
- user accounts, creating [ii-xix](#)
- User Lockout report [41-3](#)
- users
 - list of users associated with phone system [29-3](#)
 - 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 [19-6](#)
 - UndeliverableMessagesMailbox [19-6](#)
 - Unity Connection Messaging System [19-6](#)
 - user speech recognition conversation [13-3](#)

- Users report [41-1](#)
- user to user voice messages [19-2](#)
- user workstations, setting up [ii-xix](#)
- utilities and tools
 - Bulk Administration Tool [3-2](#)
 - Bulk Edit [3-3](#)
 - Cisco Unified Serviceability [3-8](#)
 - Cisco Voice Technology Group Subscription Tool [3-7](#)
 - 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 [3-1](#)
 - RTMT [3-7](#)
 - Synch Users [3-4](#)
 - Task Management [3-7](#)

V

- ViewMail for Microsoft Outlook, integrated messaging example [20-2](#)
- voice commands, using [13-3](#)
- voice messages
 - delivery [19-9](#)
 - dispatch messages [19-6](#)
 - interviews [19-3](#)
 - live record [19-4](#)
 - notifications [19-3](#)
 - outside caller [19-1](#)
 - receipts [19-3](#)
 - system broadcast [19-2](#)
 - user to user [19-2](#)
- voice messaging port
 - adding [29-17](#)
 - changing settings [29-18](#)

- deleting [29-18](#)
- voice recognition
 - allowing users to say their voice mail passwords [14-10](#)
 - Grammar Statistics tool [3-4](#)
- Voice Recognition Update schedule [10-1](#)
- VPIM contacts
 - after creating [34-10](#)
 - correcting CSV errors for Bulk Administration Tool [34-8](#)
 - creating [34-6](#)
 - creating by using Bulk Administration Tool [34-8](#)
 - creating by using CSV files [34-7](#)
 - creating with Bulk Administration Tool [34-7](#)
 - creating with Connection Administration [34-9](#)
 - customizing directory update settings [34-11](#)
 - deleting [34-14](#)
- VPIM locations
 - adding alternate names [34-13](#)
 - and Digital Networking [33-24](#)
 - creating [34-6](#)
 - customizing [34-6](#)
- VPIM Networking
 - adding alternate names for VPIM locations [34-13](#)
 - adding VPIM contacts with Connection Administration [34-9](#)
 - addresses [34-17](#)
 - addressing options [34-17](#)
 - after creating VPIM contacts [34-10](#)
 - audio formats [34-18](#)
 - configuring remote voice messaging system [34-14](#)
 - creating VPIM contacts [34-6](#)
 - creating VPIM contacts with Bulk Administration Tool [34-7, 34-8](#)
 - creating VPIM locations [34-6](#)
 - customizing VPIM contact directory update settings [34-11](#)
 - customizing VPIM locations [34-6](#)
 - deleting VPIM contacts [34-14](#)
 - design decisions [34-3](#)

- DNS [34-4](#)
- messages [34-16](#)
- messaging similarities and limitations [34-17](#)
- overview [34-1](#)
- prerequisites [34-2](#)
- removing a VPIM location [34-15](#)
- resolving names with IP addresses [34-4](#)
- sample message [34-16](#)
- setting up [34-1](#)
- setup procedures [34-3](#)
- using CSV files for creating VPIM contacts [34-7](#)
- verifying connectivity with remote voice messaging system [34-5](#)

W

- Wallet Card Wizard [3-10](#)
- warning prompt for end of recording, configuring [19-5](#)
- Weekdays schedule [10-1](#)

