



## **Cisco Unity System Administration Guide (With IBM Lotus Domino)**

Release 4.0(3)  
September 5, 2003

### **Corporate 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: 408 526-4100

Text Part Number: OL-4760-01



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

*Cisco Unity System Administration Guide (With IBM Lotus Domino)*  
Copyright © 2003, Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>xv</b>
Purpose	xv
Audience	xv
Document Conventions	xv
Cisco Unity Documentation	xvi
Obtaining Documentation	xvi
Cisco.com	xvi
Documentation CD-ROM	xvii
Ordering Documentation	xvii
Documentation Feedback	xvii
Obtaining Technical Assistance	xvii
Cisco TAC Website	xviii
Opening a TAC Case	xviii
TAC Case Priority Definitions	xviii
Obtaining Additional Publications and Information	xix

---

**CHAPTER 1**

<b>Introduction</b>	<b>1-1</b>
Cisco Unity Features	1-1

---

**CHAPTER 2**

<b>Accessing the Cisco Unity Administrator</b>	<b>2-1</b>
Accessing and Exiting the Cisco Unity Administrator	2-1
Logging On to the Cisco Unity Administrator	2-1
Exiting the Cisco Unity Administrator	2-3
Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator	2-3
About Cisco Unity Administrator Authentication	2-5
How Integrated Windows Authentication for the Cisco Unity Administrator Works	2-7
How Anonymous Authentication for the Cisco Unity Administrator Works	2-8
Changing the Authentication Method Used by the Cisco Unity Administrator	2-9
Cisco Unity Administrator Accounts	2-11
About the Accounts That Can Be Used to Administer Cisco Unity	2-11
Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator	2-12
Defining Subscriber Account Policies for Logons, Passwords, and Lockouts	2-15
Granting Administrative Rights to Other Cisco Unity Servers	2-15

**CHAPTER 3**

**Using the Cisco Unity Administrator 3-1**

- Cisco Unity Administrator User Interface 3-1
- Cisco Unity Data 3-1
- Navigation 3-2
- Using the Online Help 3-2
- Command Icons 3-3
- Saving Data 3-3
- Finding Records 3-4
- Adding Records 3-4
- Recording Greetings and Names 3-5

**CHAPTER 4**

**Maintaining a Cisco Unity System 4-1**

**CHAPTER 5**

**Manually Setting Up Cisco Unity to Use SSL 5-1**

- Determining Whether to Set Up Cisco Unity to Use SSL 5-1
- Manually Setting Up Cisco Unity to Use SSL 5-2
- Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain (Optional) 5-5

**CHAPTER 6**

**Default Accounts and Message Handling 6-1**

- Overview: Default Accounts and Message Handling 6-1
- Default Accounts 6-1
- Message Handling 6-2
  - How Cisco Unity Handles Subscribers Whose Mailboxes Are Full 6-3
  - How Cisco Unity Handles Messages Without a Specific Recipient 6-3
  - How Cisco Unity Handles Messages That Are Marked Private 6-4
  - How Cisco Unity Handles Messages That Are Interrupted by Disconnected Calls 6-4

**CHAPTER 7**

**Cisco Unity Conversation 7-1**

- How You Can Customize the Conversation 7-1
  - Using the Conversation Settings in the Cisco Unity Administrator to Customize the Subscriber Conversation 7-2
  - Using the Call Transfer Settings in the Cisco Unity Administrator to Customize the Subscriber and Unidentified Caller Conversations 7-3
  - Using the Message Settings in the Cisco Unity Administrator to Customize the Unidentified Caller Conversation 7-3
  - Activating Optional Conversation 1 for Subscribers 7-3
  - Offering Subscribers Additional Caller Information Before Message Playback 7-6
  - Changing the Order for Addressing and Recording for Subscribers 7-7

Changing How Subscribers Confirm Message Addressing	7-7
How Subscribers Can Customize the Cisco Unity Conversation	7-9
About System Prompts	7-10
Recording System Greetings	7-10
Using the Media Master to Record Greetings	7-11
Using the Cisco Unity Greetings Administrator to Manage Greetings	7-11

**CHAPTER 8**

<b>Setting Up Client Applications</b>	<b>8-1</b>
Overview: Client Applications	8-1
Setting Up Subscriber Phones	8-2
Setting Up Lotus Notes with DUCS for Cisco Unity	8-2
Setting Up the Cisco Personal Communications Assistant	8-3
About Cisco Personal Communications Assistant Authentication	8-4
Defining Subscriber Account Policies for Logons, Passwords, and Lockouts	8-5
Configuring Subscriber Browsers to Use the Cisco PCA	8-5
Setting Up Recording and Playback Devices	8-6
Using the Phone as a Recording and Playback Device	8-7
Using a Microphone and Speakers as the Recording and Playback Device	8-7
Determining Recording and Playback Devices for Subscriber Use	8-7
Specifying Recording and Playback Device Preferences in Cisco Unity Applications	8-8
Using TTY Phones with Cisco Unity	8-8

**CHAPTER 9**

<b>Subscriber, Operator, and Support Desk Orientation</b>	<b>9-1</b>
Overview: Subscriber, Operator, and Support Desk Orientation	9-1
Subscriber Orientation	9-1
Operator Orientation	9-4
Support Desk Orientation	9-5

**CHAPTER 10**

<b>Enhanced Phone Security</b>	<b>10-1</b>
Overview: Enhanced Phone Security	10-1
Setting Up Enhanced Phone Security	10-2

**CHAPTER 11**

<b>Languages</b>	<b>11-1</b>
Overview: Languages	11-1
Setting Up Languages	11-1
Specifying Text to Speech Languages	11-2
Specifying Phone Languages	11-3

- Specifying GUI Languages 11-5
- TTY Overview 11-5
  - Setting Up Cisco Unity to Use the TTY Prompt Set 11-6
  - Disabling Cisco Unity Comfort Noise 11-6
  - Using the TTY Angel 11-7
  - Using NTS for Advanced TTY Features 11-8

**CHAPTER 12**

**Integrating a Fax Server with Cisco Unity 12-1**

- Overview: Fax Server Integration 12-1
- Fax Server Integration 12-2
  - Fax Server Administration 12-2
  - Sending and Receiving Faxes with an E-Mail Client 12-2
- Task List: Integrating a Fax Server 12-3

**CHAPTER 13**

**Subscriber Template Settings 13-1**

- Overview: Subscriber Template Settings 13-1
  - Predefined Templates 13-1
- Creating and Modifying Templates 13-2
- Subscriber Template Profile Settings 13-2
- Subscriber Template Account Settings 13-4
- Subscriber Template Passwords Settings 13-4
- Subscriber Template Conversation Settings 13-5
- Subscriber Template Call Transfer Settings 13-9
- Subscriber Template Greetings Settings 13-11
- Subscriber Template Caller Input Settings 13-13
- Subscriber Template Messages Settings 13-15
- Subscriber Template Distribution Lists Settings 13-17
- Subscriber Template Message Notification Settings 13-17

**CHAPTER 14**

**Class of Service Settings 14-1**

- Overview: Class of Service Settings 14-1
  - Predefined Classes of Service 14-1
- How a Class of Service Works 14-2
- Creating and Modifying Classes of Service 14-2
- Class of Service Profile Settings 14-3
- Class of Service Subscriber Settings 14-4
- Class of Service System Access Settings 14-5

Class of Service Call Transfer Settings	14-8
Class of Service Messages Settings	14-8
Class of Service Greetings Settings	14-9
Class of Service Features Settings	14-9
Class of Service Restriction Table Settings	14-10

**CHAPTER 15****Creating Subscriber Accounts 15-1**

Overview: Creating Subscriber Accounts	15-1
Before Creating Regular Subscriber Accounts	15-2
About Regular Subscriber Accounts and Data Storage	15-4
About Subscriber Accounts	15-4
About Data Storage	15-5
Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts	15-5
Importing User Data Directly from a Message Store Directory	15-5
Importing User Data from a CSV File	15-6
Running the Cisco Unity Bulk Import Wizard	15-14
Correcting Import Errors	15-15
Using the Cisco Unity Administrator to Create Individual Subscriber Accounts	15-16
Importing Existing User Data from the Message Store	15-17
After Creating Subscriber Accounts	15-18

**CHAPTER 16****Deleting Subscriber Accounts 16-1**

How to Delete a Subscriber Account	16-1
What Happens When a Regular Subscriber Account Is Deleted	16-2

**CHAPTER 17****Subscriber Settings 17-1**

Overview: Subscriber Settings	17-1
Subscriber Profile Settings	17-2
Subscriber Account Settings	17-4
Subscriber Phone Password Settings	17-5
Subscriber Private List Settings	17-6
Subscriber Conversation Settings	17-7
Subscriber Call Transfer Settings	17-11
Subscriber Greetings Settings	17-13
Subscriber Caller Input Settings	17-16
Subscriber Messages Settings	17-17
Subscriber Message Notification Settings	17-20

- Chaining Message Notification 17-21
- Cascading Message Notification 17-21
- Text Message Notifications 17-22
- Subscriber Alternate Extension Settings 17-25
- Setting Up Alternate Extensions 17-25

**CHAPTER 18**

**Public Distribution List Settings 18-1**

- Overview: Public Distribution Lists 18-1
  - Predefined Public Distribution Lists 18-1
- Creating and Modifying Public Distribution Lists 18-2
- Public Distribution List Profile Settings 18-3
- Public Distribution Lists Members Settings 18-3

**CHAPTER 19**

**Account Policy Settings 19-1**

- Overview: Account Settings 19-1
- Phone Password Restriction Settings 19-1
- Account Lockout Settings 19-3

**CHAPTER 20**

**Call Management 20-1**

- Overview: Cisco Unity Call Management 20-1
- Creating a Call Management Plan 20-2
  - Routing Callers by Using One-Key Dialing 20-2
  - Creating a Call Management Map 20-2
  - Implementing a Call Management Plan 20-3

**CHAPTER 21**

**Call Handler Settings 21-1**

- Overview: Call Handler Settings 21-1
  - Predefined Call Handlers 21-2
- Creating and Modifying Call Handlers 21-2
  - Setting Up the Cisco Unity Greetings Administrator 21-3
  - Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings 21-5
- Call Handler Profile Settings 21-5
- Call Handler Transfer Settings 21-7
- Call Handler Greetings Settings 21-10
- Call Handler Caller Input Settings 21-12
- Call Handler Messages Settings 21-13

---

**CHAPTER 22****Directory Handler Settings 22-1**

- Overview: Directory Handler Settings 22-1
- Creating and Modifying Directory Handlers 22-1
- Directory Handler Profile Settings 22-3
- Directory Handler Search Options Settings 22-5
- Directory Handler Match List Options Settings 22-6
- Directory Handler Caller Input Settings 22-8

---

**CHAPTER 23****Interview Handler Settings 23-1**

- Overview: Interview Handler Settings 23-1
  - About the Example Interview Handler 23-1
- Creating and Modifying Interview Handlers 23-2
- Interview Handler Profile Settings 23-2
- Interview Handler Questions Settings 23-4

---

**CHAPTER 24****Call Routing 24-1**

- Overview: Call Routing Tables 24-1
- How Call Routing Rules Work 24-2
- Creating and Modifying Call Routing Rules 24-3
- Direct Calls and Forwarded Calls Routing Table Settings 24-4

---

**CHAPTER 25****Restriction Tables 25-1**

- Overview: Restriction Tables 25-1
  - Predefined Restriction Tables 25-1
- How Restriction Tables Work 25-2
- Creating and Modifying Restriction Tables 25-3
- Restriction Table Settings 25-4

---

**CHAPTER 26****Reports 26-1**

- Overview: Reports 26-1
- About Report Data 26-2
- Generating Reports 26-2
- Viewing and Printing Reports 26-3
- Subscribers Report 26-4
- Subscriber Message Activity Report 26-4
- Distribution Lists Report 26-5

- Failed Login Report 26-5
- Transfer Billing Report 26-6
- Outcall Billing Report 26-7
- Administrative Access Activity Report 26-8
- Event Log Report 26-9
- Port Usage Report 26-9
- System Configuration Report 26-10
- Unresolved References Report 26-11
- Call Handler Traffic Report 26-11

**CHAPTER 27**

**Network Settings 27-1**

- Overview: Network Settings 27-1
- Primary Location Profile Settings 27-2
- Primary Location Addressing Option Settings 27-3
- Delivery Location Profile Settings 27-5
- Monitored Domain Address Books 27-5

**CHAPTER 28**

**System Settings 28-1**

- Overview: System Settings 28-1
- Configuration Settings 28-2
- Software Versions 28-4
- Recording Settings 28-4
  - Audio Codecs 28-4
- Contacts 28-5
- Phone Languages Settings 28-5
- GUI Languages Settings 28-6
- Subscriber Address Book Settings 28-7
- Schedule Settings 28-9
- Holiday Settings 28-10
- Licensing Status 28-11
- Authentication Settings 28-11
- Voice Messaging Port Settings 28-14
- Cisco CallManager Integration 28-15
- SIP Integration 28-16
- Circuit-Switched Integration 28-17
- Setting a Warning Tone for End of Recording 28-19

Enabling the Warning Tone	28-19
Customizing the Warning Tone	28-19
Remapping Extension Numbers	28-20
About the Remapping Feature	28-20
Setting Up Cisco Unity to Remap Extension Numbers	28-20
Syntax and Examples	28-22

---

**GLOSSARY**

---

**APPENDIX A**

<b>Exiting and Starting the Cisco Unity Software and Server</b>	<b>A-1</b>
Exiting the Cisco Unity Software	A-1
Shutting Down or Restarting the Cisco Unity Server	A-2
Starting the Cisco Unity Software	A-3

---

**INDEX**





## Preface

---

This preface describes the purpose, audience, and conventions of the *Cisco Unity System Administration Guide*, and provides information on how to obtain related documentation.

## Purpose

The *Cisco Unity System Administration Guide* introduces you to the Cisco Unity Administrator, which is the administration interface for Cisco Unity, and explains how to configure Cisco Unity.

The *Cisco Unity System Administration Guide* focuses on Cisco Unity. It does not provide information on Microsoft Exchange, Microsoft Windows NT, Microsoft Windows 2000, IBM Lotus Domino, or setting up the Cisco Unity server as an e-mail server.

## Audience

This guide is intended for system administrators and others responsible for managing Cisco Unity. If you are administering the Cisco Unity server, you need a working knowledge of Windows NT/2000 and of the message store (IBM Lotus Domino, Microsoft Exchange 2000, or Microsoft Exchange 5.5) in which voice messages are stored. Although knowledge of other voice messaging systems is useful, it is not required.

## Document Conventions

This guide uses the following conventions:

**Table 1** *Cisco Unity System Administration Guide Conventions*

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

**Table 1** Cisco Unity System Administration Guide Conventions

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press <b>Ctrl-Alt-Delete</b> .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make: <ul style="list-style-type: none"> <li>On menus. (Example: On the Windows Start menu, click <b>Settings &gt; Control Panel &gt; Phone and Modem Options</b>.)</li> <li>In the navigation bar of the Cisco Unity Administrator. (Example: Go to the <b>System &gt; Configuration &gt; Settings</b> page.)</li> </ul>

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

**Note**

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

**Caution**

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

## Cisco Unity Documentation

For descriptions and the URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/about/aboutdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm).

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

## Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

**Priority 1 (P1)**—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Priority 2 (P2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Priority 3 (P3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Priority 4 (P4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
<http://www.cisco.com/en/US/learning/index.html>





# Introduction

---

## Cisco Unity Features

Cisco Unity is a Windows 2000-based communications solution that brings you voice mail and unified messaging, and integrates them with the desktop applications you use every day. Cisco Unity works with IBM Lotus Domino to deliver and store all messages—voice, fax, and e-mail—giving you the ability to access all of your messages by using your desktop PC, a touchtone phone, or the Internet.

Cisco Unity is the unified messaging component within the Cisco family of AVVID (Architecture for Voice, Video and Integrated Data) offerings, and it integrates with Cisco CallManager, the call-processing component of Cisco AVVID. Although designed for a Voice over IP environment, Cisco Unity also integrates with several traditional, circuit-switched phone systems. When you are ready to transition to Voice over IP, Cisco Unity allows you to do so in stages, by setting up a dual phone system integration with both the circuit-switched phone system and Cisco CallManager.

Cisco Unity features include the following. (Your system may not include all of these features.)

### **Intelligent Voice Mail**

The Cisco Unity voice messaging capabilities allow subscribers to listen to their messages, send voice messages to other subscribers, and customize settings such as personal greetings. With Cisco Unity you can set up an automated attendant, which serves as an electronic receptionist that answers and routes incoming calls.

### **Cisco Unity Administrator**

The Web administrator allows you access to the Cisco Unity server via an intranet and remotely. Use the Cisco Unity Administrator to create or modify subscriber accounts, configure messaging options, assign classes of service, record greetings, and run reports.

### **Cisco Personal Communications Assistant**

The Cisco Personal Communications Assistant (PCA) is a website that subscribers use to access the Cisco Unity Assistant.

### **Cisco Unity Assistant**

The Cisco Unity Assistant is a website that gives subscribers the ability to customize personal settings—including recorded greetings and message delivery options—on their computers. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

**IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity**

IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity lets subscribers listen to voice messages from their IBM Lotus Notes Inbox by using VCR-style controls.

**Multiple Languages**

With multiple languages installed, you can change the language in which Cisco Unity plays system prompts to subscribers and callers. You can also choose one or more languages with which to display the Cisco Unity Administrator pages and the Help files.

**Text to Speech**

The Text to Speech feature allows you to listen to your e-mail over the phone. Cisco Unity reads the text portion of e-mail messages and provides additional information such as the name of the sender (if the sender is a subscriber), and the time and date that the message was sent.

**Third-Party Fax**

Cisco Unity supports fax servers that have dedicated fax lines set up to the fax ports on the fax server. When a third-party fax server is used with Cisco Unity, the administration of the fax server is controlled by the fax server software.

A list of officially supported fax servers that you can use with Cisco Unity can be found in *Cisco Unity System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).

**Digital Networking**

The Digital Networking feature enables subscribers to send and receive voice messages between Cisco Unity servers at different locations, between a Cisco Unity server and the Internet, and between a Cisco Unity server and another messaging system.



## Accessing the Cisco Unity Administrator

---

The Cisco Unity Administrator is a website that you use to do most administrative tasks. Administrative tasks include determining system schedules, specifying settings for individual subscribers (or for a group of subscribers by using a subscriber template), and implementing a call management plan.

See the following sections in this chapter for more information:

- [Accessing and Exiting the Cisco Unity Administrator, page 2-1](#)—This section explains how to access and exit the Cisco Unity Administrator.
- [Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator, page 2-3](#)—When multiple Cisco Unity servers are networked together, you can access the Cisco Unity Administrator on another Cisco Unity server.
- [About Cisco Unity Administrator Authentication, page 2-5](#)—This section explains the authentication methods that you can use with the Cisco Unity Administrator.
- [Cisco Unity Administrator Accounts, page 2-11](#)—This section describes the type of accounts that you can use to access the Cisco Unity Administrator, and the ways in which you create additional accounts or grant administrative rights to existing accounts so that they can be used to administer Cisco Unity. In addition, this section describes the account policy options available for Cisco Unity Administrator logons, passwords, and lockouts.

## Accessing and Exiting the Cisco Unity Administrator

To learn about accessing and exiting the Cisco Unity Administrator, see the following sections:

- [Logging On to the Cisco Unity Administrator, page 2-1](#)
- [Exiting the Cisco Unity Administrator, page 2-3](#)

## Logging On to the Cisco Unity Administrator

Although the way in which you log on to the Cisco Unity Administrator depends on the type of authentication that it uses, the account that you use to log on remains the same: you can use either the administration account that was selected when Cisco Unity was installed, or you can use an applicable Windows domain account. When the Cisco Unity Administrator uses the Anonymous authentication method, you have the additional option of using a Domino account that is associated with an applicable

Cisco Unity subscriber account to log on. For information on which accounts can be used to access the Cisco Unity Administrator, see the [“About the Accounts That Can Be Used to Administer Cisco Unity” section on page 2-11](#).

**Note**

Until you create a Cisco Unity subscriber account for the purpose of administering Cisco Unity, you must use the Windows credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

There are potential security risks if your system is configured so that you are not prompted for a name and password when you access the Cisco Unity Administrator, and if all of the following conditions exist:

- The Cisco Unity Administrator uses the Integrated Windows authentication method
- Internet Explorer is not configured to prompt for user name and password
- You logged on to Windows in a trusted domain by using either the administration account, or an applicable Windows domain account

In this situation, we recommend that you increase security by configuring the browser to prompt for a user name and password, or by locking the workstation when it is unattended.

The length of time that the browser can be left unattended before Cisco Unity automatically logs you off is governed by the Session Timeout limit specified in IIS. When the browser session times out, you must refresh the browser, and log on to the Cisco Unity Administrator again. If the Cisco Unity Administrator uses the Anonymous authentication method, you can set the session timeout value for IIS (see the [“Authentication Settings” section on page 28-11](#) for details). When the Cisco Unity Administrator uses the Integrated Windows authentication method, you must set session limits directly in IIS.

To log on to the Cisco Unity Administrator, use the applicable procedure in this section. Note that Cisco Unity does not permit more than five administrators to access the Cisco Unity Administrator at the same time.

**To Log On to the Cisco Unity Administrator When It Uses Integrated Windows Authentication**

- 
- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using either the administration account that was selected when Cisco Unity was installed or an applicable Windows domain account.
- Step 2** If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Launch System Admin**.
- If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.
- Step 3** If Internet Explorer prompts you, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed, or an applicable Windows domain account.
-

### To Log On to the Cisco Unity Administrator When It Uses Anonymous Authentication

- 
- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using any domain account that has the right to log on locally.
- Step 2** If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Launch System Admin**.
- If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.
- Step 3** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an applicable Cisco Unity subscriber account, and click **Log On**.
  - Click **Log On Using Windows Authentication**.
- Step 4** On the Cisco Unity Log On page, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed, or an applicable Windows domain account, and click **Log On**.
- 

## Exiting the Cisco Unity Administrator

### To Exit the Cisco Unity Administrator

- 
- Step 1** Click the **Log Off** button on the lower left area of the Cisco Unity Administrator page.
- Step 2** Exit Internet Explorer.
- 

## Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator

Each Cisco Unity Administrator provides links to the Cisco Unity Administrator websites on other networked Cisco Unity servers. By clicking the links, you can access subscriber accounts and other Cisco Unity objects on another Cisco Unity server simply by browsing to the Cisco Unity Administrator on the Cisco Unity server on which those accounts and objects were created.

When you want to find a subscriber account, but do not know on which Cisco Unity server in the network the account was created, you can search for it from any subscriber page in the Cisco Unity Administrator on your local Cisco Unity server by using the Find icon.

When the Cisco Unity Administrator uses the Integrated Windows authentication method, you are not required to re-enter your Windows domain account credentials when you browse to another Cisco Unity Administrator website from your local Cisco Unity server. Note that this is true only if you log on to the Cisco Unity Administrator on your local server by using the credentials of a Windows domain account that is associated with a Cisco Unity subscriber account that has appropriate class of service (COS) rights on the remote Cisco Unity server.

**Note**

COS rights specify which tasks, if any, administrators can do in the Cisco Unity Administrator. For example, some subscriber accounts can be associated with a COS that provides read-only access, or restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords. (For more information, see the [“Class of Service System Access Settings” section on page 14-5.](#))

However, when the Cisco Unity Administrator uses the Anonymous authentication method, you are prompted to enter authentication credentials regardless of the account you used to log on to the Cisco Unity Administrator on your local server. In this case, simply enter the applicable credentials for the Cisco Unity Administrator website that you want to access.

---

**To Browse to Another Cisco Unity Administrator on a Networked Cisco Unity Server**


---

- Step 1** Near the bottom of the navigation bar on the left side of the Cisco Unity Administrator interface, click **Unity Servers**. The Server Chooser page appears.
- Step 2** From the list, click the server that you want to access.
- Step 3** If prompted, enter the applicable credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server that you selected.

---

Do the following procedure to use the Cisco Unity Administrator on your local Cisco Unity server to search for subscriber accounts on other Cisco Unity servers in the network.

---

**To Search for Subscriber Accounts Created on a Cisco Unity Server Other than Your Local Cisco Unity Server**


---

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
- Step 2** Click the **Find** icon.
- Step 3** Indicate whether to search by short name, extension, first name, or last name.
- Step 4** Enter the applicable short name, extension, or name. You also can enter \* to display a list of all subscribers, or enter one or more characters or values followed by \* to narrow your search.
- Step 5** Check the **Search All Cisco Unity Servers** check box.
- Step 6** Click **Find**.
- Step 7** On the list of matches, click the name of the subscriber to display the record.
- Step 8** If prompted, enter the applicable credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server on which the subscriber account was created. The subscriber profile page is displayed in the new browser window.

---

## About Cisco Unity Administrator Authentication

By default, IIS is configured so that the Cisco Unity Administrator uses the Integrated Windows authentication method (formerly called NTLM or Windows NT Challenge/Response authentication) to authenticate the user name and password. During installation, the installer determines whether to configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method instead.

Regardless of how the installer configured IIS, you can change the authentication method that the Cisco Unity Administrator currently uses at any time. (Note that the authentication method you choose to use also applies when accessing the Cisco Unity Status Monitor.) Before you make a change, however, first discuss it with the network administrator to confirm that the method you choose aligns with the existing authentication scheme in your organization, and that it addresses security concerns for your site. In addition, consider the advantages and disadvantages of using each authentication method with the Cisco Unity Administrator, as shown in [Table 2-1](#) and [Table 2-2](#).

Refer to the Microsoft website for general information on the strengths and weaknesses of Integrated Windows and Anonymous authentication.

**Table 2-1** Using Integrated Windows Authentication with the Cisco Unity Administrator

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user.</li> <li>• Integrated Windows authentication is the default in IIS; therefore, no additional setup is required.</li> </ul>	<ul style="list-style-type: none"> <li>• Windows cannot validate the identity of a user when the user is logged on to an untrusted domain, and therefore, denies the user access to the Cisco Unity Administrator. To mitigate this problem, configure each subscriber browser to prompt for a user name and password, allowing subscribers to enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains.</li> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they will be prompted to re-enter their credentials every time that they want to use the phone as a recording and playback device for the Media Master.</li> </ul>

**Table 2-2 Using Anonymous Authentication with the Cisco Unity Administrator**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Subscribers can choose whether to enter Domino or Windows credentials on the Cisco Unity Log On page. If subscribers use Domino credentials, they do not need to have Windows domain accounts created for them. However, if subscribers have Windows domain accounts, they can use Windows credentials to access the Cisco Unity Administrator if the Domino server goes down.</li> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they can enter the applicable credentials on the Cisco Unity Log On page for the domain that the Cisco Unity server is in. Thus, you do not need to configure each subscriber browser to prompt for a user name and password, nor do you need to establish trusts across domains.</li> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they are not prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master.</li> </ul>	<ul style="list-style-type: none"> <li>• When a subscriber enters credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To solve this problem, you can set up Cisco Unity to use SSL.</li> <li>• Because Integrated Windows authentication is the IIS default, you must configure the system to use Anonymous authentication.</li> </ul>

If you decide to change the authentication method that is currently used by the Cisco Unity Administrator, see the [“Changing the Authentication Method Used by the Cisco Unity Administrator” section on page 2-9](#). For additional information on Cisco Unity authentication, see the following sections in this chapter:

- [How Integrated Windows Authentication for the Cisco Unity Administrator Works, page 2-7](#)—This section offers a high-level summary of the authentication process performed by Windows.
- [How Anonymous Authentication for the Cisco Unity Administrator Works, page 2-8](#)—This section offers a high-level summary of the authentication process performed by Cisco Unity, including a description of the credentials required by the Cisco Unity Log On page.

In addition, you may want to review the following related sections in other chapters:

- For information on using SSL to protect user credentials and subscriber data, see the [“Manually Setting Up Cisco Unity to Use SSL”](#) chapter.
- For information on how authentication works with the Cisco Personal Communications Assistant (PCA), see the [“About Cisco Personal Communications Assistant Authentication” section on page 8-4](#).

## How Integrated Windows Authentication for the Cisco Unity Administrator Works

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, Cisco Unity does not authenticate the subscriber. Instead, the identity of the user is verified by Windows, as follows:

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS indicates that it cannot authenticate the user.
4. When Internet Explorer is configured to prompt for a user name and password, it displays a dialog box and waits for the subscriber to enter the Windows domain account credentials. When the subscriber enters the credentials, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Windows domain account (based on the credentials that the subscriber entered in the dialog box).

When Internet Explorer is not configured to prompt for a user name and password, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Windows domain account (based on the credentials that the subscriber had previously entered to log on to Windows).

In neither scenario is the user password—or any representation of the password—sent across the network, because authentication relies on Windows challenge/response.

5. If Windows can confirm the identity of the Windows domain user, IIS sends the user and domain name to Cisco Unity, and the process continues with Step 6.

If Windows cannot validate the identity of the Windows domain user (as would be the case if the subscriber logged on to an untrusted domain), Internet Explorer prompts the subscriber for a user name and password. Once again, the credentials are not sent across the network; instead, Internet Explorer sends IIS an encrypted message regarding the Windows domain account based on the credentials that are entered in the dialog box.

If authentication occurs, the process continues with Step 6. However, if Windows still cannot authenticate the user, Internet Explorer displays a message indicating that access to the website is denied because the domain account is unknown.

6. Cisco Unity checks to see that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber, and that the subscriber account has COS rights to access the Cisco Unity Administrator.

If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

## How Anonymous Authentication for the Cisco Unity Administrator Works

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page, as follows:

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR\_<Computer name> account. (This is the anonymous account that IIS uses by default for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. By default, the Log On page prompts subscribers to enter the Domino credentials, as shown in [Table 2-3](#). However, subscribers can click the Log On Using Windows Authentication link provided on the Log On page to browse to another Log On page (as shown in [Table 2-4](#)) on which they can enter their Windows domain account credentials.

**Table 2-3 Cisco Unity Log On Page for Domino Credentials**

Field Name	Description
Full Name	Subscribers enter the full Lotus Notes user name that is associated with their Cisco Unity subscriber account.  The full name consists of the user name, any organizational units that the Domino Person document resides in, and the IBM Domino certifier domain. (For example, a subscriber enters Terry Campbell/Sales/Cisco.)
Password	Subscribers enter the Internet password for their Domino user account.

**Table 2-4 Cisco Unity Log On Page for Windows Credentials**

Field Name	Description
User Name	Subscribers enter the alias for the Windows domain account that is associated with their Cisco Unity subscriber account. (For example, a subscriber can enter tcampbell, or can enter the full path tcampbell@<Domain name>.)  If subscribers enter the full path, they do not need to complete the Domain field.
Password	Subscribers enter the password for their Windows domain account.
Domain	Subscribers enter the name of the domain in which their Windows domain account resides, unless they entered a full path in the User Name field, in which case they leave this field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security risk, you can set up Cisco Unity to use SSL.)

7. When the subscriber has entered Domino credentials on the Log On page, Cisco Unity searches the Domino Address Book for a Person document associated with the user name that the subscriber entered on the Log On page. When the user name is found, Cisco Unity retrieves the encrypted password from the Person document and compares it with the password that the subscriber entered on the Log On page. The process continues with Step 8.



**Note** By default, the connection between the Cisco Unity server and the Domino server is not encrypted. Refer to the Domino documentation for details on encrypting network data on a server port. It is also a good idea to discuss potential performance issues with the Domino administrator for the organization before enabling encryption on the Domino server.

When the subscriber has entered Windows credentials on the Log On page, Cisco Unity requests authentication of the credentials from Windows. The process continues with Step 9.

8. If Cisco Unity can authenticate the Domino credentials, Cisco Unity confirms that there is a subscriber account associated with the Domino Person document used to authenticate the subscriber, and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the Domino credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

9. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber, and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the Windows credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

## Changing the Authentication Method Used by the Cisco Unity Administrator

This section contains two procedures. Do the first procedure to configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method. Do the second procedure to change back to the Integrated Windows authentication method (which is the default).

### To Configure IIS So That the Cisco Unity Administrator Uses Anonymous Authentication

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click <System-name> to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Web Properties dialog box, set the authentication method:
  - a. Click the **Directory Security** tab.
  - b. Under Anonymous Access and Authentication Control, click **Edit**.
  - c. In the Authentication Methods dialog box, check the **Anonymous Access** check box.

- d. Uncheck the **Integrated Windows Authentication** check box.
  - e. Click **OK** to close the Authentication Methods dialog box.
  - f. Click **OK** to close the Web Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for SAWeb.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for Status.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.
- Step 12** Close the Internet Information Services window.
- 

### To Configure IIS So That the Cisco Unity Administrator Uses Integrated Windows Authentication

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click **<System-name>** to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Web Properties dialog box, set the authentication method:
- a. Click the **Directory Security** tab.
  - b. Under Anonymous Access and Authentication Control, click **Edit**.
  - c. In the Authentication Methods dialog box, uncheck the **Anonymous Access** check box.
  - d. Check the **Integrated Windows Authentication** check box.
  - e. Click **OK** to close the Authentication Methods dialog box.
  - f. Click **OK** to close the Web Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for SAWeb.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for Status.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.
- Step 12** Close the Internet Information Services window.
-

# Cisco Unity Administrator Accounts

See the following sections:

- [About the Accounts That Can Be Used to Administer Cisco Unity, page 2-11](#)
- [Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator, page 2-12](#)
- [Defining Subscriber Account Policies for Logons, Passwords, and Lockouts, page 2-15](#)
- [Granting Administrative Rights to Other Cisco Unity Servers, page 2-15](#)

## About the Accounts That Can Be Used to Administer Cisco Unity

To access the Cisco Unity Administrator, administrators can use one of the following accounts:

<b>Administration account</b>	This is the account that was selected during installation to administer Cisco Unity. The administration account is automatically associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator.
<b>A Windows domain account associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator</b>	<p>In order for administrators to log on to the Cisco Unity Administrator on the Cisco Unity server, this account must be a member of one of the following Admins groups, as applicable:</p> <ul style="list-style-type: none"> <li>• Domain Admins group (when the Cisco Unity server is a domain controller)</li> <li>• Local Administrators group (when the Cisco Unity server is a member server)</li> </ul> <p>Otherwise, the account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server.</p>
<b>A Domino account that is associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator</b>	This option is available only when the Cisco Unity Administrator uses the Anonymous authentication method.

Until you create a Cisco Unity subscriber account specifically for the purpose of administering Cisco Unity, you must use the Windows credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

Consider using an alternative to the administration account, if you want to do the following:

- Limit the use of the administration account. The COS assigned to the administration account has full system access rights to the Cisco Unity Administrator. This means that not only can the administration account access all pages in the Cisco Unity Administrator, but it also has read, edit, add, and delete privileges for all Cisco Unity Administrator pages.
- Ensure that there are additional accounts available, which can be used to access the Cisco Unity Administrator if the administration account is deleted or corrupted.

The Cisco Unity subscriber accounts that are used to access the Cisco Unity Administrator must have the appropriate COS rights. COS rights specify which tasks, if any, administrators can do in the Cisco Unity Administrator. For example, some subscriber accounts can be associated with a COS that provides read-only access, or restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords. (For more information, see the [“Class of Service System Access Settings”](#) section on page 14-5.) In addition to COS rights, subscriber accounts used to access the Cisco Unity Administrator must be associated with a Windows domain account when the Cisco Unity Administrator uses Integrated Windows authentication. The same is true when the Cisco Unity Administrator uses the Anonymous authentication method and administrators will use their Windows domain account credentials to access it. (When the Cisco Unity Administrator uses Anonymous authentication and administrators will use their Domino credentials to access the Cisco Unity Administrator, you do not need to create Windows domain accounts for each subscriber account that you create.)

To create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, complete the procedures in the [“Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator”](#) section on page 2-12. If you prefer not to create a specific subscriber account for each administrator who needs to access the Cisco Unity Administrator, you can use the GrantUnityAccess utility to associate one or more Windows domain accounts with a single subscriber account. You can also use GrantUnityAccess to associate the Domino account of each administrator with a subscriber account that has COS rights to the Cisco Unity Administrator on a particular server. For more information about using the GrantUnityAccess utility, see the [“Granting Administrative Rights to Other Cisco Unity Servers”](#) section on page 2-15.

As a best practice, we recommend that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator that they use to log on to the Cisco PCA to manage their own Cisco Unity accounts. In addition, they should not use Unity service accounts to administer Cisco Unity.

## Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator

How you create additional accounts that can be used to access the Cisco Unity Administrator depends on the authentication method that the Cisco Unity Administrator uses and on the credentials that subscribers use to access it.

If the Cisco Unity Administrator uses Integrated Windows authentication (the default method), use the procedures in this section to do the following tasks:

1. Create a Windows domain account.
2. If you want the administrator to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, add the Windows domain account to the applicable Admins group. (Otherwise, the administrator can access the Cisco Unity Administrator only from another computer.)
3. Create a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator.
4. Use the GrantUnityAccess utility to associate the Windows domain account with the Cisco Unity subscriber account.

If the Cisco Unity Administrator uses Anonymous authentication and if administrators will use their Domino credentials to access the Cisco Unity Administrator, do only the [“To Create the Cisco Unity Subscriber Account\(s\) That Will Be Used to Access the Cisco Unity Administrator”](#) procedure.

---

### To Create a Windows Domain Account

---

- Step 1** On the Cisco Unity server or another computer on which Active Directory Users and Computers is installed, 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 > Active Directory Users and Computers**.
  - Step 3** In the left pane, expand the domain, right-click **Users** or the organizational unit in which you want to create the account, and click **New > User**.
  - Step 4** Follow the on-screen prompts.
  - Step 5** Close **Active Directory Users and Computers**.
- 

If you want the administrator to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you must add the Windows domain account that you created in the previous procedure either to the local Administrators group (when the Cisco Unity server is a member server), or to the Domain Admins group (when the Cisco Unity server is a domain controller). Do one of the following two procedures, as applicable.

### To Add the Windows Domain Account to the Local Administrators Group (When the Cisco Unity Server Is a Member Server)

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
  - Step 2** In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.
  - Step 3** In the left pane, click **Users**.
  - Step 4** In the right pane, double-click the administration account.
  - Step 5** In the Properties dialog box, click the **Member Of** tab.
  - Step 6** Click **Add**.
  - Step 7** In the Select Groups dialog box, in the top list, double-click **Administrators**.
  - Step 8** Click **OK** to close the Select Groups dialog box.
  - Step 9** Click **OK** to close the Properties dialog box.
  - Step 10** Close the Computer Management MMC.
- 

### To Add the Windows Domain Account to the Domain Admins Group (When the Cisco Unity Server Is a Domain Controller)

---

- Step 1** On the Cisco Unity server or another server where Active Directory Users and Computers is installed, 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 > Active Directory Users and Computers**.
- Step 3** In the left pane, expand the domain, and click **Users**.
- Step 4** In the right pane, double-click the name of the administration account.

- Step 5** Click the **Members Of** tab.
  - Step 6** Click **Add**.
  - Step 7** In the Select Groups dialog box, in the top list, double-click **Domain Admins**.
  - Step 8** Click **OK** to close the Select Groups dialog box.
  - Step 9** Click **OK** to close the Properties dialog box.
  - Step 10** Close **Active Directory Users and Computers**.
- 

#### To Create the Cisco Unity Subscriber Account(s) That Will Be Used to Access the Cisco Unity Administrator

---

- Step 1** If the Domino person that you want to use to access the Cisco Unity Administrator does not already exist, create the Person document in the Domino Administrator.
  - Step 2** On the Cisco Unity server, log on to Windows by using the administration account that was selected when Cisco Unity was installed.
  - Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Launch System Admin**.
  - Step 4** If IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication and Internet Explorer is configured to prompt you for a user name and password, enter the user name and password of the administration account in the dialog box, and press **Enter**. If Internet Explorer is not configured to prompt you for a user name and password, skip to [Step 5](#).  
  
If IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, on the Cisco Unity Log On page, click **Log On Using Windows Authentication**, and then enter the user name and password of the administration account, and the domain name for the Cisco Unity server.
  - Step 5** Create a Cisco Unity subscriber account based on the Default Administrator template by importing the Person document that you created in [Step 1](#) or another Person document from Domino. (The Default Administrator template has COS rights to access the Cisco Unity Administrator.)  
  
See the “[Creating Subscriber Accounts](#)” chapter for detailed procedures for creating subscriber accounts.
- 

Because the Cisco Unity Administrator does not import Windows domain account information, the subscriber accounts that you created in the previous procedure still cannot access the Cisco Unity Administrator without corresponding Windows domain accounts (even though they have the COS rights required to access it) when either of the following statements is true:

- The Cisco Unity Administrator uses Integrated Windows authentication.
- The Cisco Unity Administrator uses Anonymous authentication and administrators will use their Windows domain account credentials to access it.

Do the following procedure to use GrantUnityAccess to associate the Windows domain account and the Cisco Unity subscriber account(s) that you created earlier in this section.

#### To Associate a Windows Domain Account with a Cisco Unity Subscriber Account

---

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, expand **Diagnostic Tools**, and double-click **Grant Unity Access** to display a command prompt window.

**Step 3** To associate a Windows domain account with a Cisco Unity subscriber account, enter:

```
GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias>
```

For example:

```
GrantUnityAccess -u UnityDomain\UnityAdmin -s UnityFullAdmin
```

---

## Defining Subscriber Account Policies for Logons, Passwords, and Lockouts

When the Cisco Unity Administrator uses the Integrated Windows authentication method (which is the default), the account policy that is specified for each Windows domain account determines the following: how Windows handles situations when users attempt to log on to Windows and repeatedly enter incorrect passwords; the number of failed logon attempts that Windows allows before the user account cannot be used to access Windows; and the length of time that a user remains locked out.

If the Cisco Unity Administrator uses Anonymous authentication, you can use the settings on the Authentication page in the Cisco Unity Administrator to customize the logon, password, and lockout policies that Cisco Unity applies when subscribers use the Cisco Unity Administrator to access Cisco Unity. Because subscribers can use either Domino or Windows credentials to log on to the Cisco Unity Administrator, you can specify two logon and lockout policies on the Authentication pages: one that applies when subscribers use their Windows domain credentials, and another that applies when subscribers use their Domino credentials. For details, see the [“Authentication Settings” section on page 28-11](#).

## Granting Administrative Rights to Other Cisco Unity Servers

Rather than create subscriber accounts on each server for each person who needs to administer Cisco Unity, you can use the GrantUnityAccess utility to associate any number of Windows domain accounts with a single Cisco Unity subscriber account. You can also use GrantUnityAccess to associate a Domino Person document with a Cisco Unity subscriber account. GrantUnityAccess maintains a table of the associated Windows domain accounts (or Domino Person documents) and Cisco Unity subscriber accounts, which Cisco Unity references when someone tries to access the Cisco Unity Administrator (regardless of the authentication method used by the Cisco Unity Administrator). This table is used to determine whether to permit someone access to the Cisco Unity Administrator.

Before you use GrantUnityAccess, consider the following:

- The Windows domain account(s) that you want to associate with a subscriber account must either be in the same domain as the Cisco Unity server or in a trusted domain. In addition, if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you must add the Windows domain account to the applicable Admins group (see the [“Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator” section on page 2-12](#) for a detailed procedure.) Otherwise, the domain account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server.
- You can associate multiple domain accounts with a single subscriber account.
- You can associate multiple Domino Person documents with a single subscriber account.
- You can associate Windows domain account(s) or Domino Person documents with any subscriber account, as long as the subscriber account has COS rights to access the Cisco Unity Administrator. This includes the administration account that was selected when Cisco Unity was installed.

- Because the administration account is associated with a COS that offers unlimited access to the Cisco Unity Administrator, consider associating the Windows domain account(s) or Domino account(s) used by administrators with a different subscriber account that you create on each Cisco Unity server to have more limited COS rights. In this way, you can customize the level of access for the administrators in your organization. (For more information, see the “[Class of Service System Access Settings](#)” section on page 14-5.)
- If there are several servers that the administrators need access to, you can create a batch file that contains the commands to grant access to the applicable servers. In this way, you can avoid entering the commands repeatedly.

Use the following procedure to run GrantUnityAccess. Note that you cannot run GrantUnityAccess remotely across a network, so you will need to run it on each Cisco Unity server that you want to make accessible, and for each account that you want to map. See the “[Sample GrantUnityAccess Arguments](#)” section on page 2-16 for an example of how this utility is used, and for argument syntax details.

### To Use the GrantUnityAccess Utility

- 
- Step 1** Log on to Windows on the Cisco Unity server by using either the administration account that was selected when Cisco Unity was installed or a Windows domain account that is a member of the local Administrators group on the Cisco Unity server.
- Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 3** In the left pane, expand **Diagnostic Tools**, and double-click **Grant Unity Access** to display a command prompt window.
- Step 4** To associate a Windows domain account with a Cisco Unity subscriber account, enter:

```
GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias>
```

To associate a Domino Person document with a Cisco Unity subscriber account, enter:

```
GrantUnityAccess -n "<FullName>/<CertificationAuthority>" -s
<UnitySubscriberShortName>
```

Note that the quotation marks are required around the first argument, because the full name of a Domino user will more than likely contain a space.

---

### Sample GrantUnityAccess Arguments

For example, assume that JSmith and KChen are the aliases of administrators who need access to the Cisco Unity Administrator on another Cisco Unity server, and that their Windows domain accounts are in a domain called NewYorkDomain. To associate their Windows domain accounts with the administration account that was selected when Cisco Unity was installed, run GrantUnityAccess two times as follows:

```
GrantUnityAccess -u NewYorkDomain\JSmith -s <UnitySubscriberAlias for administration
account>
```

```
GrantUnityAccess -u NewYorkDomain\KChen -s <UnitySubscriberAlias for administration
account>
```

Alternatively, if you want to associate their Domino accounts with the administration account that was selected when Cisco Unity was installed, run GrantUnityAccess two times as follows:

```
GrantUnityAccess -n "Jane Smith/MyCert" -s <UnitySubscriberAlias for administration account>
```

```
GrantUnityAccess -n "Kevin Chen/MyCert" -s <UnitySubscriberAlias for administration account>
```

Rather than specifying the administration account, you could associate the Windows domain account for Neil Jones with the subscriber account for Kelly Bader instead:

```
GrantUnityAccess -u NewYorkDomain\NJones -s KBader
```

To obtain a list of accounts that have been associated with Cisco Unity subscriber accounts, enter:

```
GrantUnityAccess -l
```

To delete an association made previously using GrantUnityAccess, enter:

```
GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias> -d
```

or enter:

```
GrantUnityAccess -n <FullName>/<CertificationAuthority> -s <UnitySubscriberShortName> -d
```

To display information about these and other arguments, enter:

```
GrantUnityAccess -?
```





# Using the Cisco Unity Administrator

## Cisco Unity Administrator User Interface

The Cisco Unity Administrator interface is divided into three areas.

<b>Navigation bar</b>	Located along the left side of the interface; contains links to categories of data pages.
<b>Page</b>	Where Cisco Unity data is entered and displayed. The page name is highlighted at the top of the page.
<b>Title bar</b>	Displays the name of the record or of the group of settings that appears on the page. The title bar also features command icons that initiate actions such as saving and finding records.

## Cisco Unity Data

The Cisco Unity Administrator features links from the main navigation bar to five groupings of data, representing subscribers and other Cisco Unity entities.

The data groupings available from the Cisco Unity Administrator include:

### Subscribers

These pages are used to enter data related to individual subscriber records. Also included are subscriber template pages, which contain settings that are applied to groups of subscribers. Settings include schedules, passwords, account permissions, call processing and transfer options, and distribution lists.

### Call Management

These pages are used to set how Cisco Unity answers, routes, transfers, and records calls. Settings include call routing, prerecorded caller interviews, call recording, and allowing or blocking certain dial strings.

### Reports

These pages are used to generate reports on subscriber-based and system-based data. Reports can be generated for any of the data stored in the system, such as subscriber message activity, distribution lists, phone logons, disk storage, administration access, and port usage.

**Network**

These pages are used to add and view information about other Cisco Unity locations. Note that the network data pages are available only when Digital Networking is installed.

**System**

These pages are used to customize and view numerous system features, including business schedules, annual holidays, recording settings, and languages.

## Navigation

There are two levels of navigation in the Cisco Unity Administrator.

- At the first level, the navigation bar displays the data categories and provides links to each group of pages within those categories.
- At the second level, the navigation bar provides a link to each page within a selected group. Once a page is displayed, you can access individual records of that page type by clicking the Find icon. For more information, see the [“Finding Records” section on page 3-4](#).

Always use the Cisco Unity navigation bar, rather than the Internet Explorer navigation buttons, to move between pages. Otherwise, incorrect data may be displayed.

## Using the Online Help

The Cisco Unity Administrator includes two types of context-sensitive online Help:

<b>Online Documentation</b>	Displays Help for the current page in the Cisco Unity Administrator, and links to additional topics.
<b>Field Help</b>	Displays descriptions of individual fields in the Cisco Unity Administrator.

### To Display Online Documentation

- 
- Step 1** Click the **Online Documentation** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays the relevant page from the *Cisco Unity System Administration Guide* in a separate window.
- Step 2** If desired, click a link included in the displayed topic or listed in the Contents to browse to additional topics.
- 








### To Display Field Help

- 
- Step 1** Click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays a question mark next to each field for which Help is available.
- Step 2** For help on a field, click the question mark next to that field.

- Step 3** To turn Field Help off, click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator.

## Command Icons

The command icons are located in the title bar, which is in the upper-right area of each Cisco Unity Administrator page.

	<b>Save icon</b>	Saves data that you have entered. Available only when you have changed the record.
	<b>Find icon</b>	Opens the Find window, where you search for existing records in the displayed category.
	<b>Add icon</b>	Opens the Add window, where you enter information to create a new record in the displayed category.
	<b>Delete icon</b>	Deletes the displayed record.
	<b>Run icon</b>	Generates a report. Available only on Reports pages.
	<b>Online Documentation icon</b>	Provides in-depth descriptions and conceptual Help and includes an index and glossary.
	<b>Field Help icon</b>	Displays question marks next to fields and buttons for which Help is available.

## Saving Data

Save newly entered data by clicking the Save icon. Cisco Unity requires you to save new data before moving to another record or to another part of the Cisco Unity Administrator. The following cues remind you when the displayed record contains unsaved data:

- The Save icon is enabled.
- An asterisk is displayed on the title bar next to the record name.
- If you attempt to leave a changed record without saving it, Cisco Unity prompts you to save the record.

## Finding Records

A record is the group of settings or collection of data for an individual subscriber, class of service (COS), or other Cisco Unity entity. For example, a subscriber record contains the subscriber account data.

### To Find a Subscriber Record

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Indicate whether to search by short name, extension, first name, or last name.
  - Step 4** Enter the applicable short name, extension, or name. You also can enter \* to display a list of all subscribers, or enter one or more characters or values followed by \* to narrow your search.
  - Step 5** To search for subscriber accounts that were created on a Cisco Unity server other than your local Cisco Unity server, check the **Search All Cisco Unity Servers** check box.
  - Step 6** Click **Find**.
  - Step 7** On the list of matches, click the name of the subscriber to display the record.
- 

### To Find Other Types of Records

- 
- Step 1** In the Cisco Unity Administrator, go to any page of the applicable record type.
  - Step 2** Click the **Find** icon.
  - Step 3** Enter the applicable name. You also can enter \* to display a list of all records, or enter one or more characters followed by \* to narrow your search.
  - Step 4** Click **Find**.
  - Step 5** On the displayed list, double-click the applicable record.
- 

## Adding Records

Always enter information for a new record in an Add window.



### Caution

Entering new record information on an existing page will change the displayed record rather than create a new record.

Use the following procedure to add a record, such as a new class of service (COS), distribution list, or call handler. To add a new subscriber, see the [“Creating Subscriber Accounts”](#) chapter.

### To Add a Record

- 
- Step 1** Click the **Add** icon from any COS, distribution list, or call handler page.
  - Step 2** In the window that is displayed, enter basic identifying information, such as the name of the record.

- Step 3** Indicate whether this record is new or based on an existing one. If based on an existing record, click the name of that record on the list.
- Step 4** Click **Add**.

## Recording Greetings and Names

You can record names for subscribers, public distribution lists, private lists, and call handlers (including interview handlers and directory handlers), and greetings for subscribers and call handlers, from pages within the Cisco Unity Administrator. You can also record greetings for call handlers by using the Cisco Unity phone conversation.

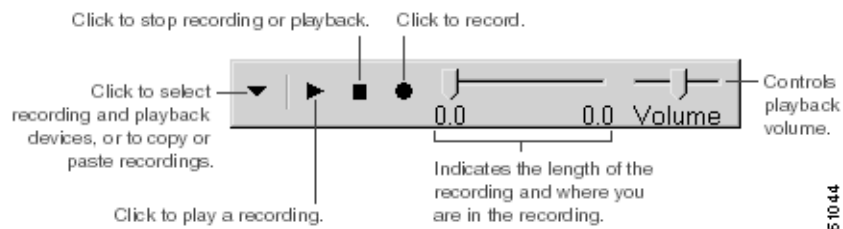
Subscribers can also record their own names and personal greetings by accessing the Cisco Unity conversation by phone, or the Cisco Unity Assistant website. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.) For more information on setting up subscribers to record, see the [“Setting Up Recording and Playback Devices”](#) section on page 8-6.

Before you begin recording subscriber and call handler names and greetings, consider the following:

- Who will record the greetings? For example, do you want to hire a professional to record the call handler greetings?
- What will the greetings say? Write detailed scripts for the greetings before beginning to record.
- Will you use the phone or a computer microphone to make and play your recordings? The phone offers the best sound quality for recordings.

The Media Master control bar appears on each page of the Cisco Unity Administrator where 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. The Media Master control bar relies on DCOM (Distributed Component Object Model), and does not work through a firewall. It also requires that your browser is able to download and run ActiveX controls.

**Figure 3-1 Media Master Control Bar**



When determining the recording and playback device that you want to use to manage greetings and subscriber names in the Cisco Unity Administrator, consider the following:

- The phone serves as the default recording and playback device for the Media Master.
- In order to use the phone as a recording and playback device, Cisco Unity must have at least one port assigned for a TRAP Connection per session on the System > Ports page. See the [“Voice Messaging Port Settings”](#) section on page 28-14 for more information.

Use the following procedure to change the recording and playback device used by the Media Master.

#### To Select a Recording and Playback Device

- 
- Step 1** Go to any Media Master control bar in the Cisco Unity Administrator.
- Step 2** From the Options menu, click **Playback Devices**.
- The Options menu button is on the far left of the Media Master control bar. See [Figure 3-1](#).
- Step 3** Select the device that you want to use from the list.
- The <Use Preferred Device> option refers to the recording and playback devices that you have already selected for your computer (click Settings > Control Panel > Sounds and Multimedia on the Windows Start menu to set your preferred devices). See the Windows online Help for more information on preferred recording and playback devices.
- Step 4** From the Options menu, click **Recording Devices**, and repeat [Step 3](#).
- 

**Table 3-1 Media Master Control Bar Options Menu**

Option	Meaning
New	Use this option to start a new recording.
Paste	Paste a copied recording of a voice message, name, or greeting into this recording.
Paste from file	Paste a WAV file that you have stored on your computer into this recording.
Copy	Copy this recording so that you can paste it into another voice message, name, or greeting recording.
Copy to file	Save this recording as a WAV file to a location that you specify.
Playback devices	Select the phone or the multimedia speakers used with your computer. If you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name.
Recording devices	Select the phone or the multimedia microphone used with your computer. Note that if you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name. Use the phone to get the best sound quality.
Options	Enter an extension and the Cisco Unity server name here when you want to use the phone as the playback and recording device for the Media Master.



## Maintaining a Cisco Unity System

---

Detailed information about maintaining a Cisco Unity system can be found in the *Cisco Unity Maintenance Guide*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/maint/maint403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint403/dom/index.htm).





## Manually Setting Up Cisco Unity to Use SSL

The procedures in the *Cisco Unity Installation Guide* for installing Cisco Unity include a partially automated process for setting up Cisco Unity to use SSL. This chapter describes the manual process to do the same operation, and helps you determine whether you should set up Cisco Unity to use SSL.

### Determining Whether to Set Up Cisco Unity to Use SSL

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true when the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method. In addition, the information that subscribers enter on the pages of the Cisco PCA and the Cisco Unity Administrator is not encrypted, regardless of which authentication method it uses.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol, if the Cisco Unity installer has not already done so during installation.

SSL uses public-key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers, or servers and clients. A digital certificate is a file containing encrypted data that attests to the identity of an organization or entity, such as a computer. Use of the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator or the Cisco PCA—are encrypted as the data is sent across the network. In addition, when Cisco Unity is set up to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected to the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a Certificate Authority (CA), or use Microsoft Certificate Services (available with Windows) to issue your own certificate. A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity. Cost, certificate features, ease of setup and maintenance, and the security policies practiced by your organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Microsoft Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

This chapter contains procedures for using Microsoft Certificate Services to issue your own certificate, and for setting up Cisco Unity to use it. See the following sections in this chapter for more information:

- [Manually Setting Up Cisco Unity to Use SSL, page 5-2](#)
- [Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain \(Optional\), page 5-5](#)

# Manually Setting Up Cisco Unity to Use SSL

To use Microsoft Certificate Services to issue your own certificate and to enable Cisco Unity to use SSL, do the procedures in this section in the order listed. Note that Microsoft Windows and IIS online documentation offer procedures similar to the ones presented in this section. The Microsoft documentation also contains procedures on how to install, configure, and use Certificate Services, and to enable a web server to use SSL in alternative ways—some of which may be more applicable to your organization than the method presented here.

Alternatively, if you purchased a certificate from a CA, refer to the procedures provided by the CA rather than the procedures in this section to set up a web server to use it.

## To Install the Microsoft Certificate Services Component

- 
- Step 1** On the server that will function as your Certificate Authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
  - Step 2** Click **Add/Remove Windows Components**.
  - Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When a warning appears about not being able to rename the computer, or join or be removed from a domain, click **Yes**.
  - Step 4** Click **Next**.
  - Step 5** Click **Stand-alone Root CA**, and click **Next**.  
A stand-alone CA is a CA that does not require Active Directory.
  - Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.  
If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the service.
  - Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
  - Step 8** Close the Add/Remove Programs dialog box and the Control Panel.
- 

## To Create a Certificate Request

- 
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
  - Step 2** Expand <System-name>.
  - Step 3** Right-click **Default Web Site**, and click **Properties**.
  - Step 4** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
  - Step 5** Under Secure Communications, click **Server Certificate**.
  - Step 6** On the Web Server Certificate Wizard welcome window, click **Next**.
  - Step 7** Click **Create a New Certificate**, and click **Next**.
  - Step 8** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
  - Step 9** Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Larger bit lengths may decrease performance.

- Step 10** Click **Next**.
- Step 11** Enter the organization information, and click **Next**.
- Step 12** For the common name of the site, enter either the Cisco Unity server system name or the fully-qualified domain name.



---

**Caution** The name entered must exactly match the host portion of any URL that will access this system by using a secure connection.

---

- Step 13** Click **Next**.
- Step 14** Enter the geographical information, and click **Next**.
- Step 15** Specify the certificate request file name and location, and click **Next**.  
Save the file to a disk or to a directory that the Certification Authority server can access.
- Step 16** Verify the request file information, and click **Next**.
- Step 17** Click **Finish** to close the Web Server Certificate Wizard.
- Step 18** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 19** Close the Internet Services Manager.

---

#### To Submit the Certificate Request

---

- Step 1** On the CA server, on the Windows Start menu, click **Run**, and then run **certreq**.
- Step 2** Browse to the directory where you saved the certificate request file in [Step 15](#) of the previous procedure, and double-click it.
- Step 3** Click the CA to use, and click **OK**.

---

By default, when the CA processes the certificate request, it assigns a pending status for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate on the virtual directories that will use it. The following two procedures guide you through the process.

#### To Issue the Certificate

---

- Step 1** On the CA server, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, expand Certification Authority, and expand <Certification Authority name>.
- Step 3** Click **Pending Requests**.
- Step 4** In the right pane, right-click the request, and click **All Tasks > Issue**.
- Step 5** In the left pane, click **Issued Certificates**.
- Step 6** In the right pane, double-click the certificate to open it.

- Step 7** Click the **Details** tab.
  - Step 8** In the Show list, choose **All**, and click **Copy to File**.
  - Step 9** On the Certificate Export Wizard welcome window, click **Next**.
  - Step 10** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
  - Step 11** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
  - Step 12** Verify the settings, and click **Finish**.
  - Step 13** Click **OK** to close the Certificate Details dialog box.
  - Step 14** Close the Certification Authority window.
- 

### To Install the Certificate

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
  - Step 2** Expand <System-name>.
  - Step 3** Right-click **Default Web Site**, and click **Properties**.
  - Step 4** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
  - Step 5** Under Secure Communications, click **Server Certificate**.
  - Step 6** On the Web Server Certificate Wizard welcome screen, click **Next**.
  - Step 7** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
  - Step 8** Browse to the directory of the certificate (.cer) file, and double-click it.
  - Step 9** Verify the certificate information, and click **Next**.
  - Step 10** Click **Finish** to close the Web Server Certificate Wizard window.
  - Step 11** Click **OK** to close the Default Web Site Properties dialog box.
  - Step 12** Close Internet Services Manager.
- 

### To Enable IIS to Use SSL

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Expand <System-name>, and expand Default Web Site.
- Step 3** Right-click **Web**, and click **Properties**.
- Step 4** In the Web Properties dialog box, click the **Directory Security** tab.
- Step 5** Under Secure Communications, click **Edit**.
- Step 6** Check the **Require Secure Channel (SSL)** check box.
- Step 7** Click **OK** to close the Secure Communications dialog box.
- Step 8** Click **OK** to close the Web Properties dialog box.
- Step 9** Under Default Web Site, right-click **Jakarta**, and click **Properties**.

- Step 10** In the Properties dialog box, click the **Directory Security** tab.
  - Step 11** Under Secure Communications, click **Edit**.
  - Step 12** Check the **Require Secure Channel (SSL)** check box.
  - Step 13** Click **OK** to close the Secure Communications dialog box.
  - Step 14** Click **OK** to close the Jakarta Properties dialog box.
  - Step 15** Close Internet Services Manager.
- 

## Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain (Optional)

When Cisco Unity is set up to use SSL, the Cisco Unity Administrator, Status Monitor, and Cisco PCA web applications automatically use an SSL connection every time a subscriber points the browser to their respective websites. An SSL connection means that Cisco Unity offers the digital certificate that you issued in the [“Manually Setting Up Cisco Unity to Use SSL”](#) section as proof of its identity each time the subscriber tries to access the Cisco Unity Administrator, Status Monitor, or the Cisco PCA. Until the certificate is added to the trusted root store on the subscriber computer, the browser will display a message to alert the subscriber that the authenticity of the site cannot be verified and, therefore, its content cannot be trusted.

You can distribute the certificate to the trusted root store for all users in the domain by adding it to the Group Policy. Before doing so, discuss it with the network administrator for your organization. If this solution is not acceptable, you can tell subscribers how to add the certificate to the trusted root store on their own computers. (This can be done later when you set up subscribers to use the Cisco PCA, as described in the [“Configuring Subscriber Browsers to Use the Cisco PCA”](#) section on page 8-5.)

Do the following two procedures in the order listed.

### To Export the CA Root Certificate

---

- Step 1** On the CA server, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, right-click <Root Certification Authority name>, and click **Properties**.
- Step 3** Click **View Certificate**.
- Step 4** Click the **Details** tab.
- Step 5** In the Show list, choose **All**, and click **Copy to File**.
- Step 6** On the Certificate Export Wizard welcome screen, click **Next**.
- Step 7** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
- Step 8** Specify a file name, and a location, and click **Next**. The location must be accessible to the Domain Admin account that will modify the group policy.
- Step 9** Verify the settings, and click **Finish**.
- Step 10** Click **OK** to close the Certificate Details dialog box.
- Step 11** Click **OK** to close the Properties dialog box for the Root Certification Authority.

**Step 12** Close the Certification Authority window.

---

#### To Add the Root Certificate to the Domain Group Policy for Trusted Root Certificate Authorities

---

- Step 1** On the CA server, 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 **Run**, and then run **mmc**.
- Step 3** On the top menu, click **Console**.
- Step 4** Click **Add/Remove Snap-in**.
- Step 5** On the Standalone tab, click **Add**.
- Step 6** In the Add Standalone Snap-in dialog box, click **Group Policy**, and click **Add**.
- Step 7** Click **Browse**.
- Step 8** In the Browse for a Group Policy Object dialog box, click the **Domains/OUs** tab.
- Step 9** In the Look In list, select the domain to which the Cisco Unity server belongs.
- Step 10** In the Domains, OUs, and Linked Group Policy Objects list, click **Default Domain Policy**, and click **OK**.
- Step 11** Click **Finish**.
- Step 12** Close the Add Standalone Snap-in dialog box.
- Step 13** Click **OK** to close the Add/Remove Snap-in dialog box.
- Step 14** In the left pane of the console window, expand **Default Domain Policy** for the Cisco Unity server domain.
- Step 15** Click **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.
- Step 16** Right-click **Trusted Root Certification Authorities**, and click **All Tasks > Import**.
- Step 17** On the Certificate Import Wizard welcome screen, click **Next**.
- Step 18** Browse to the location of the saved Root Certification Authority certificate, and double-click it.
- Step 19** Click **Next**.
- Step 20** Accept the default for the certificate store, and click **Next**.
- Step 21** Verify the settings, and click **Finish**.
- Step 22** Save the console settings.
- Step 23** Close the console window.
-



## Default Accounts and Message Handling

### Overview: Default Accounts and Message Handling

Cisco Unity uses default accounts to provide example configurations for a subscriber and for an administrator; to provide an owner for default entities involved in message handling, such as call handlers and distribution lists; and to serve as members of default classes of service.

See the following sections in this chapter for more information:

- [Default Accounts, page 6-1](#)
- [Message Handling, page 6-2](#)

### Default Accounts

During the installation of Cisco Unity, the installer is asked to choose the account that will be used to administer Cisco Unity. The purpose of this account is to allow administrator access to the Cisco Unity Administrator for initial setup. (See the [“About the Accounts That Can Be Used to Administer Cisco Unity”](#) section on page 2-11 for more information on administrative accounts.)

In addition to the account used to access the Cisco Unity Administrator, Cisco Unity creates several other default accounts and public distribution lists that you use when setting up the system. The Cisco Unity default accounts are detailed below. For a description of the default public distribution lists, see the [“Message Handling”](#) section on page 6-2 and the [“Subscriber Template Distribution Lists Settings”](#) section on page 13-17.

#### Example Administrator

The Example Administrator account, which Cisco Unity creates during installation, demonstrates the properties of an administrator account, and serves as a default owner, message recipient, and member of the following Cisco Unity entities:

- Unaddressed Messages distribution list
- All Subscribers distribution list
- System Event Messages distribution list (by default the Example Administrator is the only member of this distribution list)
- Operator call handler (by default the Example Administrator is the only member of this distribution list)
- Opening Greeting call handler
- Goodbye call handler

- Example Interview call handler
- Default Directory handler
- Default Administrator Class of Service (by default the Example Administrator is the only account with this Class of Service)

The account short name is EAdmin. The default extension is 99999. The Example Administrator has a Domino Person document and a Windows domain account, but does not have a phone password, as logging on to Cisco Unity by phone is not allowed for this account.

The Example Administrator subscriber account can not be deleted from the Cisco Unity Administrator. In fact, the account includes the instructions “Do Not Delete” as part of the subscriber name. However, the account can be deleted if necessary, by using SQL and Domino tools. For example, you might want to delete the account if the licensed subscriber limit has been reached, or if the account is perceived to be a security hazard even with a strong password.

**Caution**

Do not delete the Example Administrator account unless you have finished assigning the appropriate subscriber(s) or public distribution list(s) as message recipients or members (as applicable) of the Cisco Unity entities with which the account is associated. For more information on the impact of deleting the Example Administrator account, see the [“Deleting Subscriber Accounts”](#) chapter.

**Unity Messaging System**

The Unity Messaging System acts as a surrogate sender for messages from unidentified callers (external callers and anyone calling Cisco Unity from an internal extension that is not associated with a subscriber account, such as a conference room). Thus, subscriber messages from unidentified callers are identified as coming from the Unity Messaging System mailbox. This account also receives nondelivery receipts (NDRs) for voice messages that cannot be delivered, which it then forwards to the public distribution list called Unaddressed Messages.

The short name for this account is Unity\_<Servername>. The account cannot be seen in the Cisco Unity Administrator, but the account is created and the associated Domino Person document appears in the Domino Administrator. This account does not have a phone password, as logging on to Cisco Unity by phone is not allowed for this account. The mailbox has the display name Unity Messaging System.

**Example Subscriber**

The Example Subscriber account provides an example of typical subscriber settings; it is assigned to the default subscriber class of service. The account short name is ESubscriber. The default extension is 99990. You may delete this account at any time.

**Note**

Beginning with Cisco Unity version 4.0(3), the Example Subscriber account is no longer created during Cisco Unity installation. However, you may still have an Example Subscriber account if you upgraded from an earlier version of Cisco Unity, as the account is not removed during the upgrade process.

## Message Handling

See the following sections:

- [How Cisco Unity Handles Subscribers Whose Mailboxes Are Full, page 6-3](#)—This section describes how Cisco Unity handles full mailboxes.

- [How Cisco Unity Handles Messages Without a Specific Recipient, page 6-3](#)—This section describes how Cisco Unity handles messages that are not associated with a specific recipient, and what you must do to make sure that messages are properly routed to the applicable subscriber or call handler.
- [How Cisco Unity Handles Messages That Are Marked Private, page 6-4](#)—This section describes how Cisco Unity handles messages that are marked private.
- [How Cisco Unity Handles Messages That Are Interrupted by Disconnected Calls, page 6-4](#)—This section describes how to change the way that Cisco Unity handles messages when calls are disconnected while subscribers are in the process of sending, replying to, or forwarding a message.

## How Cisco Unity Handles Subscribers Whose Mailboxes Are Full

IBM Lotus Domino allows you to set database size quotas for user mail files. If a mail file exceeds its storage quota, a warning message is sent, and can be seen in the Misc Events view of Log.nsf. Even though a mail file has exceeded the storage quota, the router still delivers mail and the subscriber can still retrieve and send messages.

## How Cisco Unity Handles Messages Without a Specific Recipient

In some situations, messages left in Cisco Unity are not associated with a specific recipient; these messages must be screened and routed to the applicable subscriber or call handler. A subscriber should be assigned the responsibility of reviewing these messages frequently.

Such messages are left as follows:

### Unaddressed Messages Distribution List

Messages that cannot be delivered because the network or a server assigned to a subscriber goes down are forwarded to the Unaddressed Messages distribution list. By default, this distribution list contains the Example Administrator as its only member.

To route these messages properly, ensure that the Unaddressed Messages distribution list has at least one member (such as the operator) who will monitor the mailbox and handle messages that cannot be delivered. (See the [“Adding Subscribers to a Distribution List” section on page 6-4](#) for instructions.)

### System Event Messages Distribution List

The System Event Messages distribution list can be used to send event notification messages from the Event Monitoring Service (EMS). Note that by default, the System Event Messages distribution list is set up to contain the Example Administrator as its only member. To send these messages to system administrators, remove Example Administrator from the distribution list and add the appropriate subscribers to the list (see the [“Adding Subscribers to a Distribution List” section on page 6-4](#) for instructions). For information on setting up the EMS, refer to the “Configuring Cisco Unity for Maintenance Tasks” chapter in the *Cisco Unity Maintenance Guide*. The *Cisco Unity Maintenance Guide* is available at

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/maint/maint403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint403/dom/index.htm).

### Operator, Opening Greeting, and Goodbye Call Handlers

When a caller to Cisco Unity 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. Call transfer settings in the Opening Greeting and Goodbye call handlers also can allow callers to leave a message. By default,

messages left in any of these call handlers are sent to the Unaddressed Messages distribution list. For more information on call handler message recipient settings, see the [“Call Handler Messages Settings” section on page 21-13](#).

### Example Interview

When callers are routed to the Example Interview, which gathers basic information about who they are and who they are trying to reach, the answers to the questions are routed by default to the Example Administrator. If you want these messages to be routed to another recipient, choose a subscriber (such as the operator) or a distribution list as the recipient. For information on choosing an interview response recipient, see the [“Overview: Interview Handler Settings” section on page 23-1](#).

## Adding Subscribers to a Distribution List

### To Add Subscribers to the Unaddressed Messages or System Event Messages Distribution Lists

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Double-click the **Unaddressed Messages** or **System Events Messages** distribution list.
  - Step 4** Change settings as applicable, and then click the **Save** icon.
- 

## How Cisco Unity Handles Messages That Are Marked Private

Messages marked private cannot be forwarded by phone. This includes any voice message that a Cisco Unity subscriber marked private, and as applicable, any e-mail message that a subscriber or another sender marked with the “Do Not Copy” mail option in IBM Lotus Notes.

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

You can change how Cisco Unity handles messages that are interrupted by disconnected calls as subscribers are in the process of sending, replying to, or forwarding messages. Calls can be intentionally or unintentionally disconnected—for example, when a subscriber hangs up or when a cell phone loses its charge or signal.

By default, Cisco Unity sends a message when the call is disconnected in the following circumstances:

<b>When a subscriber is replying to or sending a message</b>	As long as the message has at least one recipient and the recording is more than one second (1,000 ms) in length. This means that Cisco Unity sends the message even though the subscriber may not have finished recording or addressing the message.
<b>When a subscriber is forwarding a message</b>	As long as the message has at least one recipient. This means that Cisco Unity sends the message even though the subscriber may not have recorded an introduction or completely addressed the message.

By using the Advanced Settings Tool to change the registry, you can set Cisco Unity so that it will delete interrupted messages unless subscribers have pressed the # key to send their messages. Thus, if a call is disconnected before a subscriber has a chance to press #, Cisco Unity deletes the message rather than sending it.

How Cisco Unity handles a message interrupted by a disconnected call depends on the registry value you set:

<b>0</b>	Cisco Unity sends the interrupted message even if the subscriber has not pressed the # key.
<b>1</b>	Cisco Unity deletes the interrupted message unless the subscriber has pressed the # key.

The registry change is applied systemwide to all subscribers associated with the Cisco Unity server. You cannot make the change for an individual subscriber or a specific group of subscribers.

Do the following procedure to change how Cisco Unity handles messages when calls are disconnected.

#### To Change How Cisco Unity Handles Messages Interrupted by Disconnected Calls

- 
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
  - Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
  - Step 3** In the Cisco Unity Settings pane, click **Subscriber Send Message Hang-Up Action**.
  - Step 4** In the New Value list, click the applicable value, and click **Set**.
  - Step 5** When prompted, click **OK**.
  - Step 6** Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

---





## Cisco Unity Conversation

---

When callers access Cisco Unity by phone, they hear a set of prerecorded instructions and options known as the Cisco Unity conversation—or the TUI (telephone user interface). Unidentified callers hear the unidentified caller conversation, which enables them to access the Cisco Unity automated attendant, conduct subscriber searches by using directory assistance, use call routing options, and play audiotext messages. Subscribers hear the subscriber conversation, which enables them to enroll as new subscribers, send and receive messages, record greetings, and change their personal settings.

Each Cisco Unity conversation consists of a collection of system prompts and greetings. To learn more, see the following sections in this chapter:

- [How You Can Customize the Conversation, page 7-1](#)
- [How Subscribers Can Customize the Cisco Unity Conversation, page 7-9](#)
- [About System Prompts, page 7-10](#)
- [Recording System Greetings, page 7-10](#)

### How You Can Customize the Conversation

You can customize the conversation that subscribers and unidentified callers hear in several ways. (Unless otherwise indicated, the customizations described here apply to both the standard conversation and Optional Conversation 1.)

#### Customizing the Subscriber Conversation

- You can use the conversation settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator to dictate some of what subscribers hear and how they hear it. For details, see the [“Using the Conversation Settings in the Cisco Unity Administrator to Customize the Subscriber Conversation”](#) section on page 7-2.
- You can use the call transfer settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator to dictate some of what subscribers hear when Cisco Unity transfers a call from an unidentified caller to a subscriber. For details, see the [“Using the Call Transfer Settings in the Cisco Unity Administrator to Customize the Subscriber and Unidentified Caller Conversations”](#) section on page 7-3.
- As an alternative to the Cisco Unity standard conversation, you can activate Optional Conversation 1 so that subscribers hear message-retrieval menus that may more closely resemble the choices that they are familiar with. For details, see the [“Activating Optional Conversation 1 for Subscribers”](#) section on page 7-3. (This section also contains a procedure for customizing the action that Cisco Unity takes when subscribers press # to skip a new message.)

- You can enable Cisco Unity to provide subscribers with additional information about callers who leave messages for them. For details, see the [“Offering Subscribers Additional Caller Information Before Message Playback”](#) section on page 7-6.
- You can change the order in which Cisco Unity prompts subscribers to address and record messages. For details, see the [“Changing the Order for Addressing and Recording for Subscribers”](#) section on page 7-7.
- You can alter how Cisco Unity prompts a subscriber to confirm message addressing. For details, see the [“Changing How Subscribers Confirm Message Addressing”](#) section on page 7-7.

#### Customizing the Unidentified Caller Conversation

- You can use the call transfer settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator to dictate some of what unidentified callers hear when Cisco Unity transfers a call from an unidentified caller to the subscriber. For details, see the [“Using the Call Transfer Settings in the Cisco Unity Administrator to Customize the Subscriber and Unidentified Caller Conversations”](#) section on page 7-3.
- You can use the message settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator to specify what the conversation allows unidentified callers to do when they leave messages for subscribers. For details, see the [“Using the Message Settings in the Cisco Unity Administrator to Customize the Unidentified Caller Conversation”](#) section on page 7-3.

## Using the Conversation Settings in the Cisco Unity Administrator to Customize the Subscriber Conversation

The conversation settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator allow you to dictate some of what subscribers hear and how they hear it. Some of the customizations that you can make by using the conversation settings include:

- Set volume level, and select the language in which Cisco Unity plays instructions to the subscriber.
- Specify which conversation style subscribers hear. You can also specify whether subscribers hear the comprehensive instructions offered by the full menus or brief menus for each conversation style.
- Enable Cisco Unity to play a prompt that reminds subscribers when their alternate greeting is turned on.
- Determine whether subscribers address messages to other subscribers by entering extensions, by spelling first names, or by spelling last names.
- Dictate how messages are presented to subscribers over the phone. For example, you can specify whether subscribers hear the Message Type menu, message counts, and timestamps when they check messages, and you can specify the order in which Cisco Unity plays messages.
- Select the destination—such as a call handler, interview handler, subscriber, or directory assistance—that Cisco Unity sends subscribers to when they exit the subscriber conversation.

See the [“Subscriber Template Settings”](#) or the [“Subscriber Settings”](#) chapter, as applicable, for details on using conversation settings.

You can also use the subscriber template and individual subscriber pages to specify which conversation style subscribers hear. For information on using Optional Conversation 1 versus the standard conversation, see the [“Activating Optional Conversation 1 for Subscribers”](#) section on page 7-3.

## Using the Call Transfer Settings in the Cisco Unity Administrator to Customize the Subscriber and Unidentified Caller Conversations

Some of the call transfer settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator allow you to dictate some of what subscribers and unidentified callers hear when Cisco Unity transfers calls from unidentified callers to subscriber phones. For example, depending on how you set up Cisco Unity and the phone system to handle call transfers, you may be able to use call transfer settings to:

- Select what Cisco Unity says and does when the subscriber phone is busy. You can choose to have Cisco Unity play a prompt indicating that the extension is busy and put the caller on hold, prompt the caller to leave a message and allow the caller to dial another extension, or have Cisco Unity offer the caller the option of holding, leaving a message, or dialing another extension.
- Determine what Cisco Unity plays when transferring calls from unidentified callers to the subscriber phone. You can have Cisco Unity say “transferring call,” “call for <Subscriber recorded name>,” or “call for <Dialed extension number>” when the subscriber answers the phone. You can also specify that Cisco Unity always prompts unidentified callers to say their names before Cisco Unity transfers the call so that when the subscriber answers the phone, the subscriber hears “Call from <Name of unidentified caller>,” and have Cisco Unity prompt the subscriber to accept or refuse a call from an unidentified caller.

See the “[Subscriber Template Settings](#)” or the “[Subscriber Settings](#)” chapter, as applicable, for details on using call transfer settings.

## Using the Message Settings in the Cisco Unity Administrator to Customize the Unidentified Caller Conversation

Some of the message settings on the subscriber template and individual subscriber pages in the Cisco Unity Administrator allow you to dictate some of what unidentified callers hear and how they hear it. Some of the customizations that you can make by using the message settings include:

- Specify which language that callers hear when they leave messages for subscribers.
- Specify a maximum recording length for messages from unidentified caller, and whether a warning tone is played before the caller reaches it.
- Determine which action Cisco Unity performs for unidentified callers when the subscriber phone is busy. You can specify that Cisco Unity place the caller on hold, prompt the caller to hold or leave a message, or send the caller directly to the subscriber greeting.
- Dictate whether the Cisco Unity conversation offers callers the opportunity to edit the messages that they leave for subscribers, and allows them to mark messages urgent.

See the “[Subscriber Template Settings](#)” or the “[Subscriber Settings](#)” chapter, as applicable, for details on using message settings.

## Activating Optional Conversation 1 for Subscribers

Cisco Unity Optional Conversation 1 provides an alternative to the standard conversation. You may choose to use Optional Conversation 1 because the options in its message-retrieval menus more closely resemble the options that subscribers in your organization are familiar with. Other menus—those that

unidentified callers and Cisco Unity subscribers use to send and manage messages, as well as the menus that subscribers use to change their Cisco Unity settings—are the same as those in the Cisco Unity standard conversation.

The *Cisco Unity at a Glance for Optional Conversation 1* card provides a diagram of the Cisco Unity phone conversation and is intended for subscriber use. The *Cisco Unity at a Glance for Optional Conversation 1* card is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/maint/maint403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint403/dom/index.htm).

To activate Optional Conversation 1 for individual subscribers or for a specific group of subscribers, you use the conversation settings on the applicable subscriber or template pages in the Cisco Unity Administrator.

For more details on using Optional Conversation 1 with Cisco Unity, refer to the *White Paper: Using Optional Conversation 1 with Cisco Unity Version 4.0(3)*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/whitpaper/cnv1\\_403.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpaper/cnv1_403.htm). The white paper also includes a list of caveats associated with using Optional Conversation 1.

If you choose to activate Optional Conversation 1, consider the following:

- As with the standard conversation, deleting or customizing Cisco Unity prompts is not supported.
- Changes you make to subscriber settings in the Cisco Unity Administrator are preserved after failover and upgrades; you do not need to re-activate Optional Conversation 1 in either instance.

You can use the following procedures to activate Optional Conversation 1 for a group of subscribers and for individual subscribers:

- Do the procedure, “[To Activate Optional Conversation 1 in a Subscriber Template](#)” to activate Optional Conversation 1 for a group of subscribers that you plan to create. (Changes to settings in a template do not affect any of the existing subscriber accounts that were based on that template.)
- Do the procedure, “[To Activate Optional Conversation 1 for an Existing Subscriber](#)” to specify Optional Conversation 1 for a single, existing subscriber. (If you want to activate Optional Conversation 1 for an existing group of subscribers, use the Bulk Edit tool available in Tools Depot. To do so, refer to the online Help in the applicable tool for details.)
- If you are interested in customizing Optional Conversation 1, do the procedure “[To Change How Cisco Unity Handles Messages That Subscribers Skip By Pressing # During Message Playback](#).”

#### To Activate Optional Conversation 1 in a Subscriber Template

- 
- Step 1** In the Cisco Unity Administrator, go to any Subscribers > Subscriber Template page, and find the template that you want to modify.
- Step 2** Browse to the **Conversation** page.
- Step 3** Under Phone Menu Options, click **Optional Conversation 1** from the Conversation Style menu.
- Step 4** Click the **Save** icon.
- 

#### To Activate Optional Conversation 1 for an Existing Subscriber

- 
- Step 1** In the Cisco Unity Administrator, go to any Subscribers > Subscribers page and find the subscriber whose conversation style you want to change.
- Step 2** Browse to the **Conversation** page.

- Step 3** Under Phone Menu Options, click **Optional Conversation 1** from the Conversation Style menu.
- Step 4** Click the **Save** icon.

---

You can customize Optional Conversation 1 to change how Cisco Unity handles new messages that subscribers skip during message playback. By default, when subscribers press # to skip a new message during message playback, Cisco Unity saves the message as new. This means that when subscribers call Cisco Unity to check messages, the skipped message remains in the list of new messages that Cisco Unity plays. In addition, message waiting indicators (MWI) on subscriber phones remain lit as long as there are new messages.

By using the Advanced Settings Tool to change the registry, you can customize Optional Conversation 1 so that Cisco Unity saves new messages that subscribers skip by pressing # during message playback as saved messages rather than as new messages. Subscribers in your organization may prefer this so that when they call Cisco Unity to check for new messages, they hear only newly arrived messages, and not the messages that they skipped earlier. Likewise, subscribers can then rely on their MWIs to determine when a new message arrives.

How Cisco Unity saves new messages that subscribers skip depends on the registry value you set:

<b>0</b>	Cisco Unity saves skipped messages as new messages.
<b>1</b>	Cisco Unity saves skipped messages as saved messages.

The registry change is applied systemwide to all subscribers who are associated with the Cisco Unity server and who use Optional Conversation 1. You cannot make the change for an individual subscriber or a specific group of subscribers who use Optional Conversation 1. The change does not affect subscribers who use the standard conversation.

Do the following procedure if you would like Cisco Unity to save new messages as saved messages when subscribers skip them by pressing # during message playback. Note that the procedure does not change how Cisco Unity saves messages when subscribers press 9 or # after message playback.

#### To Change How Cisco Unity Handles Messages That Subscribers Skip By Pressing # During Message Playback

- 
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Cisco Unity Settings pane, click **Optional Conversation 1: Customize Skipped Message State**.
- Step 4** In the New Value list, click the applicable value, and click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

---

## Offering Subscribers Additional Caller Information Before Message Playback

The Cisco Unity subscriber conversation can be customized so that it provides subscribers with additional information about each caller who left a message before it plays the message. By using the Bulk Edit utility (available in Tools Depot), you can provide individual subscribers or a specific group of subscribers with additional information on one or both of the types of callers who leave messages for them, as indicated in [Table 7-1](#).

**Table 7-1** Caller Information That Cisco Unity Can Offer Before Message Playback

For Messages Left By This Type of Caller	Message Type	Cisco Unity Plays This By Default	Cisco Unity Plays This When Additional Caller Information Is Offered
Identified subscriber (including call handlers)	Voice, fax, e-mail, receipts	The recorded name of the subscriber. If the subscriber (or call handler) does not have a recorded name, Cisco Unity plays the primary extension associated with the subscriber or call handler instead.	Both the recorded name (if available) and the primary extension before playing the message.  When a subscriber (or call handler) does not have a recorded name nor an extension, Cisco Unity simply plays the message without announcing who it is from.
Unidentified 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 Cisco Unity subscribers with additional caller information before message playback, consider the following requirements:

- Subscribers hear sender information before Cisco Unity plays each message only if their accounts are configured to play it. Either a Cisco Unity administrator or a subscriber can specify message playback preferences. (Cisco Unity administrators specify whether subscribers hear sender information before message playback on the Conversation pages in the Cisco Unity Administrator, while subscribers can specify their own message playback preferences in the Cisco Unity Assistant.)
- In addition, to allow Cisco Unity to provide the phone number (ANI or caller ID) information on unidentified callers, your phone system must support sending such information to Cisco Unity. (Refer to your phone system documentation for more information.) When Cisco Unity receives ANI information on a caller, it will make use of only the valid numbers, and ignores any other characters that the phone system sends.

Refer to the online Help available in Bulk Edit for details on using it to modify existing subscriber accounts. You use one or both of the following fields on the Conversation tab in Bulk Edit to offer subscribers additional caller information before message playback:

<b>Announce Sender's Extension for Messages from Subscribers</b>	Specifies whether Cisco Unity provides subscribers with additional caller information on subscribers (and call handlers) who leave messages for them.
<b>Announce ANI for Messages from Unidentified Callers</b>	Specifies whether Cisco Unity provides subscribers with additional caller information on unidentified callers who leave messages for them.

## Changing the Order for Addressing and Recording for Subscribers

The Cisco Unity subscriber conversation can be customized to change the order in which Cisco Unity prompts subscribers to address and record when they send or forward messages to other subscribers or distribution lists. By default, when a subscriber sends or forwards a message, Cisco Unity first prompts the subscriber to address the message and then prompts the subscriber to record the message or to record an introduction for a forwarded message.

By using the Advanced Settings Tool to change the registry, you can customize the subscriber conversation so that Cisco Unity prompts subscribers to record a message or introduction before prompting them to address it.

How Cisco Unity prompts subscribers to address and record when they send and forward messages depends on the registry value you set:

<b>0</b>	Cisco Unity records the message and then addresses it.
<b>1</b>	Cisco Unity addresses the message and then records it.

The registry change is applied systemwide to all subscribers associated with the Cisco Unity server. You cannot make the change for an individual subscriber or a specific group of subscribers. Finally, note that you cannot change the order in which Cisco Unity prompts subscribers to address and record when they reply to messages; Cisco Unity always prompts subscribers to record a reply before allowing them to add additional recipients.

Do the following procedure to change the order in which Cisco Unity prompts subscribers to address and record when they send messages.

### To Change the Order of Addressing and Recording When Subscribers Send Messages

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Subscriber Send Message Flow**.
- Step 4** In the New Value list, click the applicable value, and click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

## Changing How Subscribers Confirm Message Addressing

The Cisco Unity subscriber conversation can be customized to alter how Cisco Unity prompts a subscriber to confirm message addressing. By default, when a subscriber addresses a message, Cisco Unity plays the recorded name and extension of the intended recipient (or, when there is no recorded name, Cisco Unity plays the extension instead) and asks the subscriber to confirm that the recipient is correct.

By using the Advanced Settings Tool to change the registry, you can customize how Cisco Unity prompts subscribers to confirm message addressing. Table 7-2 shows the confirmation prompts that subscribers hear during message addressing, depending on the registry value you set.

**Note**

The Advanced Settings Tool also allows you to customize other aspects of the subscriber conversation. The Cisco Unity prompts listed in Table 7-2 assume that all other registry settings related to the subscriber conversation are set to their default values. Changes to some registry settings—such as the Directory List Selection Style setting—affect what the subscriber hears when you customize message addressing.

**Table 7-2 Confirmation Prompts During Message Addressing**

Registry Value	When There Is an Exact Match	When There Is More Than One Matching Name
0	“For <recipient name> at <extension>, press #. To cancel, press *.”	“There are <x> matching names; choose by number. For Alex Campbell at extension 2015, press 1. For Li Campbell at extension 2003, press 2. For Terry Campbell at extension 2078, press 3...”
1	“For <recipient name>, press #. To cancel, press *.”	“There are <x> matching names; choose by number. For Alex Campbell, press 1. For Li Campbell, press 2. For Terry Campbell, press 3...”
2	“Added.”	“There are <x> matching names; choose by number. For Alex Campbell at extension 2015, press 1. For Li Campbell at extension 2003, press 2. For Terry Campbell at extension 2078, press 3...”

The registry change is applied systemwide to all subscribers associated with the Cisco Unity server. You cannot change how Cisco Unity prompts an individual subscriber or a specific group of subscribers to confirm message addressing.

Do the following procedure to change how subscribers confirm message addressing.

#### To Change How Subscribers Confirm Message Addressing

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Subscriber Addressing Confirm Match Mode**.
- Step 4** In the New Value list, click the applicable value, and click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

# How Subscribers Can Customize the Cisco Unity Conversation

Subscribers can customize the Cisco Unity conversation by phone or by using the Cisco Unity Assistant.

Table 7-3 details the conversation settings that subscribers can change.

**Table 7-3 Settings That Subscribers Can Change**

Settings That Can Be Changed in the Cisco Unity Assistant	Settings That Can Be Changed in the Phone Conversation
Greetings: <ul style="list-style-type: none"> <li>• Record a personal greeting</li> <li>• Enable or disable greeting</li> <li>• Switch between system prompt and personal greeting</li> </ul>	Greetings: <ul style="list-style-type: none"> <li>• Record a personal greeting</li> <li>• Enable or disable greeting</li> </ul>
Call Holding and Screening: <ul style="list-style-type: none"> <li>• Select the action that Cisco Unity performs for unidentified callers when the subscriber 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</li> <li>• Select the action that Cisco Unity performs when the subscriber answers calls from unidentified callers, including telling the subscriber who the call is for, announcing that Cisco Unity is transferring the call, prompting the subscriber to accept or refuse a call, and prompting callers to say their names</li> </ul>	Call Holding and Screening: None
Message Playback: <ul style="list-style-type: none"> <li>• Select full or brief Cisco Unity conversation menus</li> <li>• Select the action that Cisco Unity performs when the subscriber calls Cisco Unity, including greeting the subscriber by name and announcing the number of new messages by type</li> <li>• Select the action that Cisco Unity performs when messages are played, including announcing the name and number of the sender who left a message, whether the timestamp is played before or after the message, and the volume level at which messages are played</li> </ul>	Message Playback: Select full or brief Cisco Unity conversation menus
Message Addressing: <ul style="list-style-type: none"> <li>• Switch between addressing messages to other subscribers by name, or by extension<sup>1</sup></li> <li>• Specify order for addressing messages by name (last name followed by first name, or vice versa)</li> </ul>	Message Addressing: Switch between addressing to other subscribers by name or by extension (by pressing ##)
Caller Options: <ul style="list-style-type: none"> <li>• Allow callers to edit messages</li> <li>• Allow callers to mark messages urgent</li> </ul>	Caller Options: None

Table 7-3 Settings That Subscribers Can Change (continued)

Settings That Can Be Changed in the Cisco Unity Assistant	Settings That Can Be Changed in the Phone Conversation
Personal Settings: <ul style="list-style-type: none"> <li>Record a name</li> <li>Change directory listing status</li> <li>Select the language used for the subscriber phone conversation</li> </ul>	Personal Settings: <ul style="list-style-type: none"> <li>Record a name</li> <li>Change directory listing status</li> </ul>

1. Note that this depends on whether you have enabled spelled name addressing. See the “[Configuration Settings](#)” section on page 28-2 for details.

To set up the recording and playback devices that subscribers will use, see the “[Setting Up Recording and Playback Devices](#)” section on page 8-6. For a complete list of settings that subscribers can change by phone or in the Cisco Unity Assistant—including call transfer, message notification, and private list settings, see the “[Subscriber Orientation](#)” section on page 9-1.

## About System Prompts

System prompts are standard recordings that come with the Cisco Unity system, and they cannot be changed by using the Cisco Unity Administrator, the Cisco Unity Assistant, or the phone conversation.

System prompts are played in different combinations in multiple places in the phone conversation. All system prompts are located in the `CommServer\Localize\Prompts` directory and subdirectories.

Do not delete system prompts, as this can cause system errors. Customizing system prompts is not supported. All system prompts are automatically deleted and replaced whenever you upgrade Cisco Unity, including maintenance upgrades.

## Recording System Greetings

You can record names for subscribers, public distribution lists, private lists, and call handlers (including interview handlers and directory handlers), and greetings for subscribers and call handlers, from pages within the Cisco Unity Administrator. In addition, when you cannot access the Cisco Unity Administrator, you can access the Cisco Unity Greetings Administrator from any phone to manage greetings for call handlers.

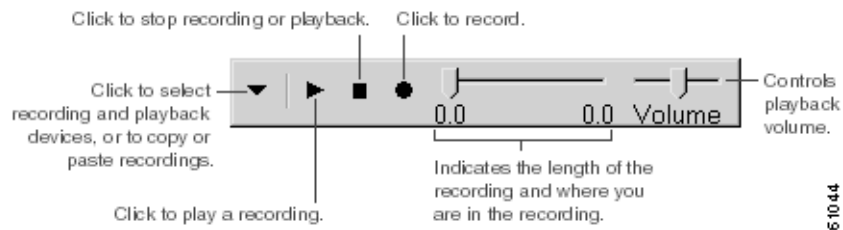
Before you begin recording subscriber and call handler names and greetings, consider the following:

- Who will record the greetings? For example, do you want to hire a professional to record the call handler greetings?
- What will the greetings say? Write detailed scripts for the greetings before beginning to record.
- Will you use the phone or a computer microphone to make and play your recordings? The phone offers the best sound quality for recordings.

## Using the Media Master to Record Greetings

The Media Master control bar appears on each page of the Cisco Unity Administrator where 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.

**Figure 7-1 Media Master Control Bar**



For additional information on determining or selecting the recording and playback device for the Media Master, see the [“Recording Greetings and Names”](#) section on page 3-5.

## Using the Cisco Unity Greetings Administrator to Manage Greetings

The Cisco Unity Greetings Administrator allows you—or the call handler owner(s) that you assign—to manage call handler greetings from any phone. The owner of the call handler can be any subscriber or public distribution list. (Note that the call handler owner is not necessarily the message recipient.)

By using the Cisco Unity Greeting Administrator, you can do the following tasks without having to access the Cisco Unity Administrator:

- Rerecord a call handler greeting.
- Enable or disable the alternate greeting for a call handler.
- Determine which greeting is currently active for a call handler.

For example, if your office is unexpectedly closed because of bad weather, you can call Cisco Unity from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.



**Note**

The RSA SecurID system is not available for subscribers who use the Cisco Unity Greetings Administrator.

For information on setting up and using the Cisco Unity Greetings Administrator, see the [“Setting Up the Cisco Unity Greetings Administrator”](#) section on page 21-3 and the [“Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings”](#) section on page 21-5.





# Setting Up Client Applications

## Overview: Client Applications

Cisco Unity subscribers can send and manage voice, fax, and e-mail messages by using a touchtone phone or by using Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity. In addition, the Cisco Unity Assistant lets subscribers personalize the Cisco Unity phone settings that control how they interact with Cisco Unity by phone.

This chapter reviews the preparations necessary for setting up subscriber phones and workstations so that subscribers can use Cisco Unity client applications. See the following sections for details:

- [Setting Up Subscriber Phones, page 8-2](#)—This section summarizes what you must do so that subscribers can access Cisco Unity by phone.
- [Setting Up Lotus Notes with DUCS for Cisco Unity, page 8-2](#)—This section lists the tasks for setting up e-mail clients for unified messaging subscribers.
- [Setting Up the Cisco Personal Communications Assistant, page 8-3](#)—This section summarizes what you must do so that subscribers can use the Cisco Personal Communications Assistant to access the Cisco Unity Assistant.
- [Setting Up Recording and Playback Devices, page 8-6](#)—This section explains how subscribers make and play recordings from the various Cisco Unity applications, and what you need to do to set them up.

### Related Documentation

- Once you have set up subscribers to use the Cisco Unity client applications, review the tasks presented in the [“Subscriber, Operator, and Support Desk Orientation”](#) chapter to orient subscribers and operators to Cisco Unity.
- For a list of supported versions of Cisco Unity combined with the supported versions of the software on subscriber workstations, refer to the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/cmptblty/clientmx.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/clientmx.htm).
- For supported languages, refer to the *Cisco Unity System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).

## Setting Up Subscriber Phones

For each subscriber phone, do the following tasks, as applicable:

- Enable call forwarding to Cisco Unity, so that busy and unanswered calls to the subscriber extension are transferred to Cisco Unity to handle. Cisco Unity then uses the call transfer settings for each subscriber to determine, for example, whether callers are put on hold or sent directly to the subscriber greeting.
- Enable easy message access, so that the subscriber can use a “Messages” button or a similar speed-dial button on the phone to dial the internal Cisco Unity phone number for your organization. This makes calling Cisco Unity to check messages or to change personal settings by phone quick and easy for the subscriber.

You can also change the phone password for individual subscribers. By default, subscriber template settings include an initial phone password for subscribers, which is 12345. To protect Cisco Unity from unauthorized access, the default phone password should be changed. As a best practice, specify a long—eight or more digits—and non-trivial password whenever you set subscriber passwords, and if you allow subscribers to change their own passwords, encourage them to do the same. (The minimum phone password length is specified on the Subscribers > Account Policy > Phone Password Restrictions page).

If the default password has not already been changed, or if you need to reset the subscriber password for any other reason, you can do so for an individual subscribers on the Subscribers > Subscribers > Phone Password pages in the Cisco Unity Administrator. Alternatively, you can use the Cisco Unity Bulk Import wizard to change the phone passwords for multiple subscribers at the same time. (Refer to the Cisco Unity Bulk Import online Help for details.)

If their accounts are configured to allow them to do so, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Note that Internet subscribers cannot log on to Cisco Unity by phone or use the Cisco Unity Assistant.

## Setting Up Lotus Notes with DUCS for Cisco Unity

By using Lotus Notes with DUCS for Cisco Unity, Cisco Unity subscribers can send and manage voice, fax, and e-mail messages from their IBM Lotus Notes Inbox. Subscribers can use Lotus Notes with DUCS for Cisco Unity to send voice messages to other subscribers, to non-Cisco Unity subscribers, and to public distribution lists. They can play and record voice messages by using the VCR-style recording and playback controls presented in the message form.

Cisco Unity activates a message waiting indicator (MWI) on the subscriber phone whenever a subscriber receives a new voice message. After the subscriber listens to all new messages over the phone, Cisco Unity immediately turns off the MWI—unless the subscriber chooses to save a message as new—to reflect that the subscriber has no new messages. However, when a subscriber listens to new messages by using Lotus Notes with DUCS for Cisco Unity, Cisco Unity relies on the Domino server to determine whether the subscriber has listened to new messages. As a result, subscribers who work with Lotus Notes offline will report that MWIs on their phones do not turn off in a timely manner. Advise subscribers that once their Lotus Notes client replicates with the Domino server, the MWI will be turned off.

Lotus Notes with DUCS for Cisco Unity is not a licensed feature, nor does it require that you give subscribers special class of service privileges or passwords to use it. To set up Lotus Notes with DUCS for Cisco Unity, install Lotus Notes with DUCS for Cisco Unity on each subscriber workstation, as applicable. Refer to the Lotus Notes with DUCS for Cisco Unity documentation for details.

**Note**

If you are upgraded from an earlier version of Cisco Unity to Cisco Unity version 4.0(3), you must also upgrade to DUCS for Cisco Unity version 1.2 on all subscriber workstations.

## Setting Up the Cisco Personal Communications Assistant

Subscribers use the Cisco Personal Communications Assistant (PCA) to access the Cisco Unity Assistant. The Cisco Unity Assistant is a website that gives subscribers the ability to customize personal settings—including recorded greetings or message delivery options—on their workstations.

The Cisco PCA is not a licensed feature, nor are subscribers required to have class of service rights to access it. Any Cisco Unity subscriber can access the Cisco PCA at <http://<Cisco Unity server>/ciscopca>. (Note that the URL is case-sensitive.) However, subscribers do require proper class of service rights to the Cisco Unity Assistant.

**Caution**

In order for the Cisco Unity Assistant to work properly on subscriber workstations, on the Cisco Unity server you must exclude the directory in which Cisco Unity is installed (the default directory is CommServer) and all subdirectories under that directory from virus scanning. Typically, this is done during Cisco Unity installation. Refer to the online Help for the virus-scanning software for information on excluding directories from scanning.

In version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA. Subscribers who use the following ActiveAssistant URLs will be automatically redirected to the Cisco PCA website:

- <http://<Cisco Unity server>/web/aa>
- <http://<Cisco Unity server>/ActiveAssistant>

Cisco PCA is installed on the Cisco Unity server during installation. To allow subscribers to access it, you do not need to install any additional files on subscriber workstations; however, you must complete the following tasks:

1. As applicable, give subscribers proper class of service rights to the Cisco Unity Assistant. See the [“Class of Service Features Settings”](#) section on page 14-9.
2. Understand how authentication works with the Cisco PCA, and any security issues that may affect your organization. See the [“About Cisco Personal Communications Assistant Authentication”](#) section on page 8-4.
3. Confirm that you have defined an appropriate logon, password, and lockout policy for all subscribers who will access the Cisco PCA. See the [“Defining Subscriber Account Policies for Logons, Passwords, and Lockouts”](#) section on page 8-5.
4. Configure subscriber browsers to use Cisco Unity web applications. See the [“Configuring Subscriber Browsers to Use the Cisco PCA”](#) section on page 8-5.

## About Cisco Personal Communications Assistant Authentication

Cisco Unity offers application-level authentication to allow subscribers to access the Cisco Personal Communications Assistant (PCA). This means that IIS is configured so that the Cisco PCA uses Anonymous authentication, and therefore Cisco Unity authenticates the credentials that subscribers enter when they log on to the Cisco PCA. Note that unlike the Cisco Unity Administrator, you cannot change the authentication method used by the Cisco PCA.

By default, when subscribers log on to the Cisco PCA, their IBM Lotus Notes user names and Internet passwords for their Domino user accounts are sent across the network to Cisco Unity in clear text. The information that a subscriber enters on the Cisco PCA pages is also not encrypted. For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. See the “[Manually Setting Up Cisco Unity to Use SSL](#)” chapter for details.

As a best practice, we recommend that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator that they use to log on to the Cisco PCA.



### Caution

If you want to use the Upgrade to More Secure Internet Password Format option that is available in the Domino Administrator, you must install Notes version 5.0.11 or later on the Cisco Unity server. Otherwise, Cisco Unity subscribers will not be able to log on to Cisco PCA.

### How Authentication for the Cisco Personal Communications Assistant Works

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco PCA website.
2. Internet Explorer tries to get the home page for the Cisco PCA from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR\_<Computer name> account. (This is the anonymous account that by default IIS uses for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter the Domino credentials, as shown in [Table 8-1](#).

**Table 8-1** Cisco Unity Log On Page for Domino Credentials

Field Name	Description
Full Name	Subscribers enter the full Lotus Notes user name that is associated with their Cisco Unity subscriber account.  The full name consists of the user name, any organizational units that the Domino Person document resides in, and the IBM Domino certifier domain. (For example, a subscriber enters Terry Campbell/Sales/Cisco.)
Internet Password	Subscribers enter the Internet password for their Domino user account.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security risk, you can set up Cisco Unity to use SSL.)
7. Cisco Unity searches the Domino Address Book for a Person document associated with the user name that the subscriber entered on the Log On page. When the user name is found, Cisco Unity retrieves the encrypted password from the Person document and compares it with the password that the subscriber entered on the Log On page.

**Note**

By default, the connection between the Cisco Unity server and the Domino server is not encrypted. Refer to the Domino documentation for details on encrypting network data on a server port. It is also a good idea to discuss potential performance issues with the Domino administrator for the organization before enabling encryption on the Domino server.

8. If Cisco Unity can authenticate the Domino credentials, Cisco Unity confirms that there is a subscriber account associated with the Domino Person document used to authenticate the subscriber, and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco PCA website, which is displayed in the browser.

If the Domino credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco PCA website.

## Defining Subscriber Account Policies for Logons, Passwords, and Lockouts

Subscribers use their IBM Lotus Notes user names and the Internet passwords for their Domino user accounts log on to the Cisco PCA. The account policy that you specify on the Authentication page in the Cisco Unity Administrator determines how Cisco Unity handles situations when subscribers attempt to log on to the Cisco PCA and repeatedly enter incorrect passwords; the number of failed logon attempts that Cisco Unity allows before the subscriber account cannot be used to access the Cisco PCA; and the length of time that a user remains locked out.

The password for accessing the Cisco PCA is inherited from the password settings in Domino.

Subscribers cannot use the Cisco Unity phone conversation or the Cisco Unity Assistant to change their Cisco PCA passwords, nor can administrators change them in the Cisco Unity Administrator. Instead, they must use Notes to change their password. However, for increased security, you can use the settings on the Authentication pages to prohibit the use of blank passwords, even when the Domino account allows them.

To customize the logon, password, and lockout policies that Cisco Unity applies whenever subscribers use the Cisco PCA to access Cisco Unity, see the [“Authentication Settings” section on page 28-11](#).

## Configuring Subscriber Browsers to Use the Cisco PCA

To allow subscribers to access the Cisco PCA, configure their browsers to:

- Enable Active scripting
- Download and run ActiveX controls
- Enable Java scripting
- Accept all cookies

### Bookmarking Web Pages

When subscriber browser settings are set to cache temporary Internet pages automatically, subscribers can create a bookmark or Favorite to access a Cisco Unity Assistant web page, but the page will be read-only. Explain to subscribers that they should bookmark the Cisco PCA home page, rather than individual pages in the Cisco Unity Assistant.

### Using SSL

If you set up Cisco Unity to use SSL, consider that the Cisco PCA website automatically uses an SSL connection every time that a subscriber points the browser to either website. However, until the digital certificate is added to the trusted root store on the subscriber workstation, the browser will display a message to alert the subscriber that the authenticity of the site cannot be verified and therefore, its content cannot be trusted.

To prevent the browser from displaying the security alert, you can distribute the certificate to the trusted root store for all users in the domain by adding it to the Group Policy, or you can tell subscribers how to add the certificate to the trusted root store on their own workstations by providing them with the following procedure. See the “[Manually Setting Up Cisco Unity to Use SSL](#)” chapter for additional details about SSL.

Depending on your organization, it may be a good idea to provide subscribers with the following procedure even if you distributed the certificate to the trusted root store for all users in the domain, as the browser will display the security alert any time that subscribers access the Cisco PCA from a workstation that does not belong to a trusted domain (for example, from a computer at home).

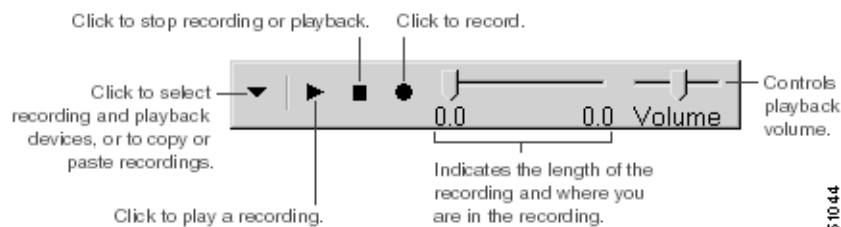
#### To Add the Cisco Unity Certificate to the Trusted Root Store on Subscriber Workstations

- 
- Step 1** On each subscriber workstation, start Internet Explorer.
  - Step 2** Go to <http://<The Certificate Authority server>/certsrv>.
  - Step 3** On the Microsoft Certificate Services page, under Select a Task, click **Retrieve the CA Certificate or Certificate Revocation List**.
  - Step 4** Click **Next**.
  - Step 5** Click the **Install This CA Certification Path** link.
  - Step 6** When prompted, click **Yes** to add the certificate to the Root Store.
- 

## Setting Up Recording and Playback Devices

Subscribers can make and play recordings in the Cisco Unity Assistant, either by using the phone, or by using the computer microphone and speakers and clicking the Media Master controls. Lotus Notes with DUCS for Cisco Unity offers a similar, VCR-style recording and playback device in the message form. Subscribers with the applicable class of service settings can also use the Media Master in the Cisco Unity Administrator to make and play recordings.

**Figure 8-1 Media Master Control Bar**



See the following sections for more information:

- [Using the Phone as a Recording and Playback Device, page 8-7](#)
- [Using a Microphone and Speakers as the Recording and Playback Device, page 8-7](#)
- [Determining Recording and Playback Devices for Subscriber Use, page 8-7](#)
- [Specifying Recording and Playback Device Preferences in Cisco Unity Applications, page 8-8](#)
- [Using TTY Phones with Cisco Unity, page 8-8](#)

## Using the Phone as a Recording and Playback Device

When subscribers use the phone as a recording and playback device in the Cisco Unity Administrator, the Cisco Unity Assistant, or Lotus Notes with DUCS for Cisco Unity, the following occurs:

- a. The subscriber clicks the applicable option in the client application to make or play a voice recording.
- b. The client application asks Cisco Unity to place a call to the subscriber extension, and Cisco Unity calls the extension.
- c. When making a recording, the subscriber answers the phone, and begins recording the message, name, or greeting. When the subscriber hangs up, the client application tells Cisco Unity that the recording is finished.

When playing a recording, the subscriber answers the phone, and the client application asks Cisco Unity to play the message. Cisco Unity streams the recording over the phone.

## Using a Microphone and Speakers as the Recording and Playback Device

When subscribers use a computer microphone and speakers as a recording and playback device in the Cisco Unity Administrator, the Cisco Unity Assistant, or Lotus Notes with DUCS for Cisco Unity, the following occurs:

- a. The subscriber clicks the applicable option in the client application to make or play a voice recording.
- b. When making a recording, the subscriber begins speaking into the microphone. When the subscriber clicks the applicable option in the client application to stop recording, the client application tells Cisco Unity that the recording is finished.

When playing a recording, Cisco Unity streams the message to the client application. Streaming occurs on demand, regardless of network traffic. The client application begins to play the message through the speakers as soon as a few seconds of the message are buffered in memory on the subscriber workstation.

## Determining Recording and Playback Devices for Subscriber Use

When determining which recording and playback devices that you want subscribers to use, consider the following:

- The phone offers the best sound quality for recordings, and serves as the default recording and playback device for the Media Master.

- In order for subscribers to use the phone as a recording and playback device, Cisco Unity must have at least one port designated for this purpose (see the [“Voice Messaging Port Settings” section on page 28-14](#) for more information). Note that when a subscriber listens to messages or other recordings by using a computer microphone and speakers, no ports are used, which decreases the load on the Cisco Unity server and leaves ports open for other functions.
- You must provide sound cards, speakers, and microphones to subscribers who do not want to use the phone as their recording and playback device.
- Media Master relies on DCOM (Distributed Component Object Model), and does not work through a firewall. Keep this in mind when setting up subscribers for remote access.

## Specifying Recording and Playback Device Preferences in Cisco Unity Applications

Subscribers can set their own recording and playback device preferences. For example, the Media Master Options menu allows subscribers to choose their own recording and playback devices. Media Master recording and playback settings are saved per user, per workstation. This means that:

- A subscriber who is logged on to the Cisco Unity Administrator or the Cisco PCA can change recording and playback devices from any Media Master Options menu. The recording and playback devices that a subscriber chooses apply to all Cisco Unity applications, as long as the subscriber accesses the applications from the same workstation on which the changes were initially made.
- If multiple subscribers share the same workstation, each subscriber who uses the workstation must indicate a choice of recording and playback devices.
- If a subscriber has updated the choice of recording and playback devices from one workstation, but also accesses the Cisco Unity Assistant, or Lotus Notes with DUCS for Cisco Unity on a different workstation (for example, from a computer at home), the choice of recording and playback devices must be indicated for the second workstation as well.

## Using TTY Phones with Cisco Unity

Beginning with Cisco Unity version 4.0(3), a TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call in to Cisco Unity and use the same features that a hearing caller can use. However, note the following exceptions:

- TTY tones are not available for use in navigating through the Cisco Unity conversation.
- Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.

For information on installing the TTY prompt set, see the [“TTY Overview” section on page 11-5](#).



# Subscriber, Operator, and Support Desk Orientation

## Overview: Subscriber, Operator, and Support Desk Orientation

Subscribers and operators in your organization need information about Cisco Unity that is specific to your installation. In addition, if your organization has a support desk, the staff will need to be prepared to answer the questions that subscribers may ask, and need to be aware of the resources that are available to assist them in answering subscriber questions. This chapter reviews the preparations for orienting subscribers, operators, and support desk employees to Cisco Unity.

See the following sections:

- [Subscriber Orientation, page 9-1](#)
- [Operator Orientation, page 9-4](#)
- [Support Desk Orientation](#)

## Subscriber Orientation

After you create subscriber accounts and set up the client applications that subscribers will use to access Cisco Unity from their computers, complete the tasks in this section to acquaint subscribers with Cisco Unity.

- Give each subscriber a *Cisco Unity User Guide*, a *Cisco Unity at a Glance* card, a *Cisco Unity Phone Menus and Shortcuts* card, and/or the URLs to the document(s).

Subscriber documentation is available at

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html).

- Give subscribers the phone numbers that they dial from inside and from outside the organization to access Cisco Unity. Also give them the name and extension of the Cisco Unity system administrator. There are spaces to record this information in the *Cisco Unity User Guide*, the *Cisco Unity at a Glance* card, and the *Cisco Unity Phone Menus and Shortcuts* card.

If you enable easy message access on subscriber phones, show them which button or key to use to access Cisco Unity.

- Provide each subscriber with a phone password. Subscriber template settings include a default phone password for subscribers, which is 12345. To protect Cisco Unity from unauthorized access, the default phone password should be changed. See the [“Subscriber Template Passwords Settings” section on page 13-4](#) for more information.

- Give subscribers the URL to the Cisco Personal Communications Assistant (PCA) website: `http://<Cisco Unity server name>/ciscopca`. Subscribers can use the Cisco PCA website to access the Cisco Unity Assistant. There are spaces to record the URL in the *Cisco Unity User Guide*, the *Cisco Unity at a Glance* card, and the *Cisco Unity Phone Menus and Shortcuts* card.  
Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA. Subscribers who use a bookmarked ActiveAssistant URL will be redirected automatically to the Cisco PCA website.
- If you have Internet subscribers in your organization, review the *Networking in Cisco Unity Guide* for information on how Cisco Unity behaves differently for these subscribers, and acquaint them with Cisco Unity accordingly. In particular, explain to subscribers the methods for addressing voice messages to other locations: over the phone, and in IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity. For detailed information, refer to the *Networking in Cisco Unity Guide*, which is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/net/net403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net403/dom/index.htm).
- If your organization has subscribers who will use TTY and the TTY prompt set, provide training on using TTY with Cisco Unity. For more information on TTY, see the “[TTY Overview](#)” section on page 11-5.
- Make sure that subscribers who own call handlers or public distribution lists understand their responsibilities (if applicable). See the “[How Cisco Unity Handles Messages Without a Specific Recipient](#)” section on page 6-3.
- Tell subscribers how to use the Cisco Unity Greetings Administrator, as applicable. See the “[Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings](#)” section on page 21-5.
- Provide training on using the phone or the Cisco Unity Assistant to personalize subscriber settings in Cisco Unity, as summarized in [Table 9-1](#). Subscribers can refer to the *Cisco Unity User Guide* or the online Help available in the Cisco Unity Assistant for further guidance after orientation.

**Table 9-1 Settings That Subscribers Can Change <sup>1</sup>**

<b>Settings That Can Be Changed By Using the Cisco Unity Assistant</b>	<b>Settings That Can Be Changed By Using the Phone Menus</b>
Greetings: <ul style="list-style-type: none"> <li>• Record a personal greeting</li> <li>• Enable or disable greeting</li> <li>• Switch between system prompt and personal greeting</li> </ul>	Greetings: <ul style="list-style-type: none"> <li>• Record a personal greeting</li> <li>• Enable or disable greeting</li> </ul>
Call Transfers: <ul style="list-style-type: none"> <li>• Transfer calls to an extension or send to the greeting</li> <li>• Change extension</li> </ul>	Call Transfers: <ul style="list-style-type: none"> <li>• Transfer calls to an extension or send to the greeting</li> <li>• Change extension</li> </ul>

**Table 9-1 Settings That Subscribers Can Change (continued)<sup>1</sup>**

<b>Settings That Can Be Changed By Using the Cisco Unity Assistant</b>	<b>Settings That Can Be Changed By Using the Phone Menus</b>
<p>Call Holding and Screening:</p> <ul style="list-style-type: none"> <li>• Select the action that Cisco Unity performs for unidentified callers when the subscriber 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</li> <li>• Select the action that Cisco Unity performs when the subscriber answers calls from unidentified callers, including telling the subscriber who the call is for, announcing that Cisco Unity is transferring the call, prompting the subscriber to accept or refuse a call, and prompting callers to say their names</li> </ul>	<p>Call Holding and Screening:</p> <p>None</p>
<p>Message Notification:</p> <ul style="list-style-type: none"> <li>• Enable or disable a notification device, and change its number</li> <li>• Specify dialing options</li> <li>• Select the types of messages and message urgency for which Cisco Unity will call a device</li> <li>• Set up a notification schedule, and specify what happens when a device does not answer, is busy, or fails</li> </ul>	<p>Message Notification:</p> <p>Enable or disable a notification device, and change its number</p>
<p>Message Playback:</p> <ul style="list-style-type: none"> <li>• Select full or brief Cisco Unity conversation menus</li> <li>• Select the action that Cisco Unity performs when the subscriber calls Cisco Unity, including greeting the subscriber by name and announcing the number of new messages by type</li> <li>• Select the action that Cisco Unity performs when messages are played, including announcing the name and number of the sender who left a message, whether the timestamp is played before or after the message, and the volume level at which messages are played</li> </ul>	<p>Message Playback:</p> <p>Select full or brief Cisco Unity conversation menus</p>
<p>Message Addressing:</p> <ul style="list-style-type: none"> <li>• Switch between addressing messages to other subscribers by name, or by extension</li> <li>• Specify order for addressing messages by name (last name followed by first name, or vice versa)</li> </ul>	<p>Message Addressing:</p> <p>Switch between addressing to other subscribers by name or by extension (by pressing ##)<sup>2</sup></p>

**Table 9-1 Settings That Subscribers Can Change (continued)<sup>1</sup>**

Settings That Can Be Changed By Using the Cisco Unity Assistant	Settings That Can Be Changed By Using the Phone Menus
Caller Options: <ul style="list-style-type: none"> <li>• Allow callers to edit messages</li> <li>• Allow callers to mark messages urgent</li> </ul>	Caller Options: None
Personal Settings: <ul style="list-style-type: none"> <li>• Record a name</li> <li>• Specify a fax delivery number</li> <li>• Change directory listing status</li> <li>• Change password</li> <li>• Select the language used for the subscriber phone conversation</li> </ul>	Personal Settings: <ul style="list-style-type: none"> <li>• Record a name</li> <li>• Specify fax delivery number</li> <li>• Change directory listing status</li> <li>• Change password</li> </ul>
Private Lists: <ul style="list-style-type: none"> <li>• Enter a display name</li> <li>• Record a name</li> <li>• Add and delete members</li> </ul>	Private Lists: <ul style="list-style-type: none"> <li>• Add and delete members</li> </ul>

1. The Conversation settings that subscribers can change are detailed in the [“How Subscribers Can Customize the Cisco Unity Conversation” section on page 7-9](#).
2. Note that this depends on whether you have enabled spelled name addressing. See the [“Configuration Settings” section on page 28-2](#) for details.

## Operator Orientation

Operator orientation should address the same points as subscriber orientation, but in greater detail. Operators must be familiar with how subscribers use Cisco Unity. Depending on the size of your organization, when subscribers have questions about Cisco Unity, the operator may be the person they are likely to ask.

In addition to the items discussed in the [“Subscriber Orientation” section on page 9-1](#) and the [“Support Desk Orientation” section on page 9-5](#) (as applicable), operators also need to understand the following concepts and tasks:

### Roles of the Operator and the Automated Attendant

The way your organization uses the automated attendant determines what the operator responsibilities are. The automated attendant is a call handler that is used in place of a human operator to answer and direct calls by playing greetings and responding to touchtones. The automated attendant can provide a menu of options (for example, “For Sales, press 1; for Service, press 2.”), and it can also provide information (for example, “Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.”).

### Directing Calls

Regardless of how your organization uses the automated attendant, many calls will go to the operator. The operator must know how to direct calls to voice mail and to subscriber phones. To direct calls to voice mail, the operator can dial Cisco Unity and at the Opening Greeting, dial the subscriber extension and then press #2. The subscriber phone does not ring, and the transferred caller hears the subscriber greeting.

You can also create a call handler for each subscriber to send calls directly to their greetings. For details on setting this up, refer to the techtip, “How to Transfer a Caller Directly into a Mailbox,” available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html).

### Forwarding Unaddressed Messages to Intended Recipients

If an operator also owns a call handler or public distribution list, make sure that the operator knows to review unaddressed messages frequently, and to forward them to the intended recipient(s). See the “[How Cisco Unity Handles Messages Without a Specific Recipient](#)” section on page 6-3.

### Using the Cisco Unity Greetings Administrator

An operator who is responsible for changing call handler greetings for the organization can use the Cisco Unity Greetings Administrator when changing a greeting in the Cisco Unity Administrator is not practical. For example, if the office is unexpectedly closed because of bad weather, the operator can call from home to use the Cisco Unity Greetings Administrator to enable the alternate Opening Greeting, or to rerecord a call handler greeting stating that the office is closed. For more information, see the “[Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings](#)” section on page 21-5.

## Support Desk Orientation

Support desk orientation should address the same points as subscriber and operator orientation, but in greater detail. Support desk staff must be familiar with how subscribers and operators use Cisco Unity.

To prepare for possible calls to the support desk at your organization, familiarize the support desk staff with the following resources and potential subscriber concerns.

### Support Desk Resources

- Subscriber documentation is available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html). In particular, support desk staff may find the *Cisco Unity at a Glance* cards helpful in gaining a high-level visual understanding of the flow of Cisco Unity conversation.
- The *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/cmptblty/clientmx.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/clientmx.htm).
- The “[Setting Up Client Applications](#)” chapter offers information on how subscriber workstations should be set up, and describes how subscribers utilize Cisco Unity tools.
- The “[Cisco Unity Conversation](#)” chapter summarizes the ways in which Cisco Unity administrators and subscribers can customize the conversation.
- The *Cisco Unity Troubleshooting Guide* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/tsg/tsg403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/tsg/tsg403/dom/index.htm).
- For descriptions and the URLs of all Cisco Unity documentation on Cisco.com, refer to *About Cisco Unity Documentation*. The document is shipped with Cisco Unity and is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/about/aboutdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm).

### Potential Subscriber Concerns

- If your organization set up Cisco Unity to use SSL, but did not add it to the Group Policy in order to distribute the certificate to the trusted root store for all users in the domain (or did not tell subscribers how to add the certificate to the trusted root store on their own computers), subscribers may be concerned about the security alert that will be displayed each time that they access the Cisco PCA. Tell them that they can ignore the warning and proceed to use the Cisco PCA without doing any harm to their computers or the network.

(To prevent the browser from displaying the security alert, see the [“Configuring Subscriber Browsers to Use the Cisco PCA”](#) section on page 8-5.)

- Subscribers may not understand that Cisco Unity and IBM Lotus Notes both handle deleted messages in the same way; thus, when subscribers delete messages over the phone, they cannot use Cisco Unity to retrieve them.
- Subscribers who work with Lotus Notes offline may not know that Cisco Unity relies on the Domino server to determine whether the subscriber has listened to new messages. Therefore, when a subscriber listens to new messages by using Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity, MWIs on subscriber phones are not turned off until the Lotus Notes client replicates with the Domino server.
- Depending on how Cisco Unity is set up at your organization, subscribers may be surprised at how Cisco Unity handles messages when calls are intentionally or unintentionally disconnected (for example, when a subscriber hangs up or when a cell phone loses its charge or signal) while subscribers are in the process of sending, replying to, or forwarding a message. See the [“How Cisco Unity Handles Messages That Are Interrupted by Disconnected Calls”](#) section in the [“Default Accounts and Message Handling”](#) chapter for details.
- If your organization has enabled the warning tone for the maximum allowable recording length, explain to subscribers that as they record messages, subscribers may wonder about the warning tone that sounds before they reach the maximum recording length. When they hear the warning tone, they must conclude the message. For more information on the warning tone, see the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19.



## Enhanced Phone Security

### Overview: Enhanced Phone Security

You can set up Cisco Unity subscriber accounts to use a secure logon method known as two-factor user authentication. Cisco Unity works with the RSA SecurID system to provide this method of enhanced phone security. The RSA SecurID system is made up of three major components: RSA SecurID authenticators, the RSA ACE/Server, and the RSA ACE/Agent.

With the RSA SecurID system, each authorized Cisco Unity subscriber is assigned an RSA SecurID authenticator. Every 60 seconds, the authenticator generates and displays a new, unpredictable number—known as a secure ID or tokencode—that is unique to the subscriber. RSA offers authenticators in the form of hardware, software, and smart cards.

Each Cisco Unity subscriber who has an authenticator must have a user account on the ACE/Server. You use the RSA Database Administrator program on the ACE/Server to create and maintain the user accounts. A user account contains the RSA alias and PIN, and information about the user authenticator. By using the information in a user account, the ACE/Server generates the same secure ID as the user authenticator.

In the Cisco Unity Administrator, you assign subscribers to a class of service for which enhanced phone security is enabled. By default, Cisco Unity uses the subscriber short name as specified in the Domino address book for the subscriber RSA alias.

When logging on to Cisco Unity over the phone, subscribers enter an ID as usual. Then, instead of a password, subscribers enter a passcode, which is a number that combines the subscriber PIN and the secure ID displayed on the subscriber authenticator. Cisco Unity uses the ID to look up the user RSA alias and sends the RSA alias and passcode to the ACE/Agent installed on the Cisco Unity server. The ACE/Agent encrypts the RSA alias and passcode and sends it to the ACE/Server. The ACE/Server looks up the user account, then validates the passcode by using the information stored in the account. The ACE/Server returns a code to the ACE/Agent, which in turn passes it along to Cisco Unity. Return code meanings are shown in [Table 10-1](#).

**Table 10-1** ACE/Server Return Codes

Return Code	Meaning
Passcode accepted	Cisco Unity allows subscriber access to messages.
Access denied	Cisco Unity prompts the subscriber to enter the passcode again. This return code can also indicate that the ACE/Server is unavailable.

Table 10-1 ACE/Server Return Codes (continued)

Return Code	Meaning
Secure ID expired	Cisco Unity prompts the subscriber to enter the next secure ID displayed on the authenticator.
New PIN needed	Cisco Unity prompts the subscriber to enter a new PIN.

Unless you have assigned PINs, the first time subscribers log on they will have not yet created PINs, so instead of passcodes, they will enter only secure IDs. The subscriber conversation guides the subscriber through the process of creating a PIN. Cisco Unity detects when New PIN mode is enabled or when a subscriber PIN has been cleared in the RSA Database Administrator, and the subscriber conversation prompts the subscriber to create a new PIN at the next logon. When subscribers log on to Cisco Unity after a PIN has been cleared, instead of a passcode, they enter only a secure ID.

**Note**

The RSA SecurID system is not available for subscribers who use the Cisco Unity Greetings Administrator. See the “[Cisco Unity Conversation](#)” chapter for information on the Cisco Unity Greetings Administrator.

## Setting Up Enhanced Phone Security

If you have an existing ACE/Server, skip the steps below that do not apply. Refer to the RSA documentation for information on setting up the ACE/Server and ACE/Agent and for creating and maintaining user accounts.

### To Set Up Enhanced Phone Security

- Step 1** Install and configure the ACE/Server. Install only the Local Access Authentication (Client) and the Control Panel Applet components. Do not install the Web Access Authentication (Server) component.
- Step 2** On the ACE/Server, use the RSA Database Administrator program to create the applicable user accounts. Note that when specifying settings for PIN assignments, indicate user-created PINs only. Cisco Unity does not support system-generated PINs.
- Step 3** Create a group that includes all the users who will use enhanced phone security on Cisco Unity.
- Step 4** Create an Agent Host for each Cisco Unity server.
- Step 5** Specify **Communications Server** as the Agent Host type.
- Step 6** Add the group you created in [Step 3](#) to the Group Activation section of the new client.
- Step 7** On each Cisco Unity server, install and configure the ACE/Agent to work with the Agent Host(s) you created on the ACE/Server.
- Step 8** Use the ACE/Agent Test Authentication utility to authenticate a user with the ACE/Server. If you cannot authenticate the user with the test program, troubleshoot the ACE client/server connection.
- Step 9** Start **Cisco Unity**.
- Step 10** In the Cisco Unity Administrator on each Cisco Unity server, go to the **System > Configuration > Settings** page and check the **RSA Two Factor** check box.
- Step 11** Log off of the **Cisco Unity Administrator**.

- Step 12** Shut down and restart each **Cisco Unity** server for enhanced phone security to take effect.
  - Step 13** Create a new class of service (COS) or modify an existing COS for the subscribers who are using enhanced phone security. (See the “[Class of Service Settings](#)” chapter for detailed procedures.)
  - Step 14** On the Subscribers > Class of Service > Profile Page of the applicable COS, click **Enhanced Security** in the Phone Security section.
  - Step 15** Assign subscribers to the enhanced phone security COS.
  - Step 16** If the RSA alias for the subscriber is something other than the short name that is specified in the Domino address book, go to the subscriber Profile page and enter the RSA alias in the Enhanced Security User Alias box.
  - Step 17** Distribute the RSA authenticators to the appropriate subscribers.
- 

#### To Disable Enhanced Security System-wide

---

- Step 1** In the Cisco Unity Administrator on each Cisco Unity server, go to the **System > Configuration > Settings** page, and uncheck the **RSA Two Factor** check box.
  - Step 2** For every class of service (COS) currently being used in your system, go to the applicable **Subscribers > Class of Service > Profile** page on the Cisco Unity server, and click **Regular Phone Security**.
-





# Languages

## Overview: Languages

The Cisco Unity Administrator provides settings for phone languages, Text to Speech (TTS), and GUI languages. Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers; TTS languages are the languages in which Cisco Unity can play e-mail messages over the phone, and GUI languages are the languages in which the Cisco Unity Administrator is displayed.

The number of language licenses available determines how many phone, TTS, and GUI languages Cisco Unity can load and use at a time. For example, if your organization has two phone language licenses, but has four languages installed, Cisco Unity will allow you to load and use only two at any one time. You can, however, select which two are used, and you can change this selection at any time. This flexibility allows you to better manage the language needs of your users.

For the complete list of supported languages for Cisco Unity, refer to the “Cisco Unity Languages” section in *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).



### Caution

Customizing system prompts is not supported for any of the Cisco Unity phone languages. All system prompts are automatically deleted and replaced whenever you upgrade Cisco Unity, including the installation of maintenance releases.

See the following sections:

- [Setting Up Languages, page 11-1](#)
- [Specifying Text to Speech Languages, page 11-2](#)
- [Specifying Phone Languages, page 11-3](#)
- [Specifying GUI Languages, page 11-5](#)
- [TTY Overview, page 11-5](#)

## Setting Up Languages

The phone, TTS, and GUI languages are chosen and installed during the initial Cisco Unity setup, and the applicable files are copied to the Cisco Unity server for each selected language.

One of the languages installed on the Cisco Unity server must match the Windows operating system locale selected during Windows installation. Additional languages may be installed as needed.

If during initial setup you did not install the language(s) you need, refer to the “Adding Languages” section in the “Modifying the Cisco Unity 4.0 System” chapter of the *Cisco Unity Installation Guide* for details on how to add or replace languages. If you are adding TTS, refer to the “Adding Text to Speech” section. (The *Cisco Unity Installation Guide* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/inst/inst403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst403/dom/index.htm).)


**Caution**

Before removing a Cisco Unity language, confirm that it is not the language that matches the Windows locale, that it is not listed in the Loaded table on the System > Configuration > Phone Languages and/or GUI Languages pages, that it is not listed as the default Phone, TTS, or GUI language, and that it is not in use by any subscriber, routing rule, call handler, interview handler, or directory handler. Do not change the Windows locale language without updating all of the locations where the corresponding Cisco Unity languages (both old and new) are specified.

In the following circumstances, if the language specified is not listed in the Loaded table on the System > Configuration > Phone Languages and/or GUI Languages pages, Cisco Unity will use the default phone, TUI, or GUI language:

- When a language is specified in a Cisco Unity component
- When a language is specified as the Windows locale

## Specifying Text to Speech Languages

The Text to Speech language engine translates e-mail text into audio, enabling subscribers to listen to e-mail by using the phone. TTS is available only with Unified Messaging.

The default TTS language is specified during installation, and can be viewed and changed on the System > Configuration > Phone Languages page.

The Cisco Unity server can support the use of multiple additional TTS language engines, as needed. All supported TTS language engines are automatically installed with the Cisco Unity software. For a complete list of supported TTS language engines, refer to the “Cisco Unity Languages” section in *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).

Use of TTS is controlled by the number of Text to Speech session licenses, and by subscriber class of service. The number of simultaneous TTS sessions on a Cisco Unity server cannot exceed the maximum number of sessions supported for the applicable platform overlay, as specified in the *Cisco Unity Supported Platforms List*. Depending on the needs of your site, you can grant TTS use to all subscriber classes of service, or limit it to specific classes of service. For more information, see the “[Class of Service Features Settings](#)” section on page 14-9. (The *Cisco Unity Supported Platforms List* is available at [http://www.cisco.com/warp/public/cc/pd/unco/un/prodlit/ucutp\\_st.htm](http://www.cisco.com/warp/public/cc/pd/unco/un/prodlit/ucutp_st.htm).)

Typically, the phone language(s) that you install and choose for use by subscribers will also be used as their TTS language(s), with the following exceptions:

- If you installed Australian English or New Zealand English as your phone language during setup, you also need to install either UK English or United States English language to serve as your default TTS language.
- There is no applicable TTS language available for Brazilian Portuguese, Czech, or Korean.
- Mainland Mandarin and Japanese TTS require specific language settings on the Cisco Unity server. If you are using either of these two languages, complete the following procedures, as applicable.

---

### To Use Mainland Mandarin Text to Speech

---

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Regional Options**.
  - Step 2** On the General tab, in the Your Locale (Location) list, click **Chinese (PRC)**.
  - Step 3** In the Language Settings for the System box, click **Simplified Chinese**.  
If you have a multi-lingual system, choose additional languages as applicable.
  - Step 4** Click **Set Default**. The Set System Locale dialog box opens.
  - Step 5** In the Select Appropriate Locale list, click **Chinese (PRC)**.
  - Step 6** Restart the Cisco Unity server for the changes to take effect.
- 

---

### To Use Japanese Text to Speech

---

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Regional Options**.
  - Step 2** On the General tab, in the Your Locale (Location) list, click **Japanese**.
  - Step 3** In the Language Settings for the System box, click **Japanese**.  
If you have a multi-lingual system, choose additional languages as applicable.
  - Step 4** Click **Set Default**. The Set System Locale dialog box opens.
  - Step 5** In the Select Appropriate Locale list, click **Japanese**.
  - Step 6** Restart the Cisco Unity server for the changes to take effect.
- 

## Specifying Phone Languages

You specify a default phone language and other system-wide phone language settings on the System > Configuration > Phone Languages page.

If desired, you can customize the language setting for individual Cisco Unity components without changing the default language settings for the rest of the system. The phone language setting is available for the following Cisco Unity components: subscriber accounts, routing rules, call handlers, interview handlers, and directory handlers. For each of these entities, you can use the pages in the Cisco Unity Administrator to specify a phone language, or you can specify that the phone language be “Inherited.”

With the Inherited setting, Cisco Unity determines the phone language to use for callers on a per-call basis, depending on how the call is processed. For example, you can set up a call handler with the Inherited language 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 Cisco Unity plays the call handler system prompts will depend on which rule routed the call. However, note that if every component in your system that processes a call has been set with Inherited as the language setting, Cisco Unity will play the system prompts in the default phone language, because in effect none of the components will have been set to a specific language.

Recorded greetings are always played in the language in use when the greeting was recorded. For example, changing the language setting for the Opening Greeting call handler from U.S. English to French will not automatically convert the greeting that was originally recorded in English to one that is played back in French. The Opening Greeting must be re-recorded in French. This is also true for subscriber greetings and for other handlers.

For more information about the settings on the Phone Languages page, see the [“Phone Languages Settings” section on page 28-5](#).

Do the procedure [“To Change Phone Language Settings for Cisco Unity Components”](#) to change the phone language settings for routing rules, call handlers, interview handlers, and directory handlers.

To specify phone language settings for individual subscribers, do the procedure [“To Change Phone Language Settings for Subscriber Accounts.”](#) To modify language settings for multiple subscriber accounts, you can use the Cisco Unity Bulk Import wizard or the Bulk Edit utility (see the [“Subscriber Settings”](#) chapter for details). Note that subscribers can use the Cisco Unity Assistant to select the language that they hear when they log on to Cisco Unity by phone.

### To Change Phone Language Settings for Cisco Unity Components

- 
- Step 1** In the Cisco Unity Administrator, go to the applicable Call Routing, Call Handler, Interview Handler, or Directory Handler page.
- Step 2** Go to following page(s), as applicable:
- For routing rules, go to the **Direct Calls** page or **Forwarded Calls** page.
  - For call handlers, go to the **Profile** page.
  - For interview handlers, go to the **Profile** page.
  - For directory handlers, go to the **Profile** page.
- Step 3** In the Language field, select one of the languages listed, or select **Inherited**.
- Step 4** Re-record applicable greetings in the new language.
- 

### To Change Phone Language Settings for Subscriber Accounts

For each subscriber account, you can specify the language in which system prompts are played to callers (this affects prompts such as “Record your message at the tone”), and you can change the language that subscribers hear when listening to the subscriber conversation.

Note that if the class of service to which a subscriber belongs has TTS, the language you select in the Subscriber’s Language field also controls the language that the TTS e-mail reader uses. Before changing the phone and TTS language for a subscriber, verify that you have the applicable languages installed. See the [“Setting Up Languages” section on page 11-1](#) for more information.

- 
- Step 1** In the Cisco Unity Administrator, go to any Subscriber page.
- Step 2** Do the following actions, as applicable:
- To change the phone language for callers, go to the **Messages** page. In the Language That Callers Hear field, select a specific language, or select **Inherited**.
  - To change the phone language for subscribers, go to the **Conversation** page. In the Subscriber’s Language field, select one of the languages listed.

- Ask the subscriber to re-record their greeting(s) in the new language.
- 

## Specifying GUI Languages

You specify a default GUI language and other system-wide GUI language settings on the System > Configuration > GUI Languages Page. To change the GUI language used in the Cisco Unity Administrator and the Cisco Personal Communications Assistant (PCA), select a language in the browser. (Subscribers use the Cisco PCA to access the Cisco Unity Assistant. Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

For the Cisco Unity Administrator, the language selected in the browser must be one of the languages in the Loaded list on the GUI Languages page. If the language that you select in the browser is not among the loaded languages, Cisco Unity uses the default GUI language; for the Cisco PCA, the language selected in the browser must be one of the languages that the Cisco PCA offers.

See the [“GUI Languages Settings” section on page 28-6](#) for more information.

## TTY Overview

With Cisco Unity version 4.0(3) and later, a TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call in to Cisco Unity and use the same features that a hearing caller can use. However, note the following limitations:

- G.711 MuLaw must be selected as the message recording and storage codec. The Cisco Unity TTY prompt set is not compatible with G.729a or other message recording and storage codecs.
- A dedicated phone number must be set up for use by outside callers with TTY. All greetings, prompts, and subscriber names accessible from this number must be created with the TTY prompt set.
- TTY is a TUI language only. At the present time, there is no compatible Text to Speech (TTS) language for TTY. The TTY prompt set is also not suitable for use as a GUI language.
- TTY tones are not available for use in navigating through the Cisco Unity conversation. Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.
- Due to recording and playback limitations, the TTY prompt set can not be used in interview handlers.

See the following sections for information on setting up and using the Cisco Unity TTY prompt set:

- [Setting Up Cisco Unity to Use the TTY Prompt Set, page 11-6](#)
- [Disabling Cisco Unity Comfort Noise, page 11-6](#)
- [Using the TTY Angel, page 11-7](#)
- [Using NTS for Advanced TTY Features, page 11-8](#)

## Setting Up Cisco Unity to Use the TTY Prompt Set

To set up Cisco Unity for TTY, do the following tasks.

1. Obtain a dial-in number that will be used exclusively for outside callers with TTY to call in to Cisco Unity. Set up the phone system and integration as required.
2. Install TTY devices for subscribers, as needed. For information about using Nix products with Cisco Unity and Cisco CallManager, see the [“Using NTS for Advanced TTY Features”](#) section on page 11-8.
3. Install the ENX language on the Cisco Unity server.
4. Confirm that G.711 is selected as the Cisco Unity message recording and storage code.
5. Disable Cisco Unity comfort noise. See the [“Disabling Cisco Unity Comfort Noise”](#) section on page 11-6.
6. Create a TTY subscriber template. This template will be used when creating subscriber accounts for all subscriber who will use TTY. You may also want to create a TTY class of service, on which you disable Text to Speech for these subscribers.
7. Create a routing rule for the TTY dial-in number.
8. Create an opening greeting call handler for the TTY dial-in number.
9. Set up additional TTY call handlers as needed.
10. Record greetings in TTY by using the TTY Angel, or by using the Media Master and a TTY phone as a recording and playback device. You will need to record the following greetings, as applicable: the opening greeting, additional call handler greetings, and subscriber greetings. See the [“Using the TTY Angel”](#) section on page 11-7.
11. Test the TTY dial-in number, opening greeting, call handlers, and all subscriber devices to confirm correct operation for both incoming and outgoing TTY calls.

## Disabling Cisco Unity Comfort Noise

Comfort noise is low-level background noise generated on a IP device. Its purpose is to simulate the hiss produced in a circuit-switched connection, and it can be generated to help provide reassurance to callers when there is no audio from Cisco Unity, for example, during a transfer or between system prompts.

The Cisco Unity ComfortNoise registry setting is a system-wide setting that controls the ability of Cisco Unity to send comfort noise generation packets to an IP phone, or to a gateway that is enabled to receive and respond to comfort noise generation packets.

If Cisco Unity comfort noise is enabled on a system that is using the TTY prompt set, TTY subscribers may report that characters are occasionally garbled or dropped. Disabling Cisco Unity comfort noise will prevent this problem from occurring.

Disabling Cisco Unity comfort noise should not cause a problem for non-TTY subscribers, but be aware that callers may notice short periods of silence between some Cisco Unity prompts.

### To Disable Cisco Unity Comfort Noise

- 
- Step 1** Start Regedit.

**Caution**

Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

- 
- Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
- Step 3** Expand the registry key  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Avaudio\Parameters\ComfortNoise.
- Step 4** In the Edit Dword Value window, click **Decimal**.  
Set the value to **128**.
- Step 5** Click **OK**.
- Step 6** Restart the Cisco Unity server.
- 

## Using the TTY Angel

The TTY prompt set includes all system prompts needed to use TTY with Cisco Unity. The TTY Angel application, available in Tools Depot, is used to create custom call handler and subscriber greetings, and subscriber recorded names, in TTY.

You can also create a CSV file containing a list of greetings and subscriber names to be converted to TTY all at once. Refer to the TTY Angel online Help for more information about this option.

### To Use the TTY Angel to Create Greetings and Recorded Names

---

- Step 1** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, expand Administrative Tools, and double-click **TTY Angel**. The TTY Angel window appears.
- Step 3** To create a new greeting or subscriber voice name, in the Output File Name window, enter a location and file name for the new TTY file.  
For example, enter C:\TTY Greetings\Opening Greeting.
- Step 4** In the Text to Convert to TTY/TDD Wav File window, enter the greeting, subscriber name, or other text as applicable, and click **Create Wav File**.  
The text is converted, displayed in the Diagnostic Output window, and stored in the designated output file and in the clipboard.
- Step 5** To paste the TTY WAV file into a call handler or subscriber record, in the Cisco Unity Administrator, browse to the applicable subscriber or call handler page.
- Step 6** On the Media Master Control Bar, click the Options menu, and click **Paste** or **Paste From File** as applicable. The WAV file is pasted into the record.
-

## Using NTS for Advanced TTY Features

NTS version 4.0 and later, available from NXi Communications, is compatible with Cisco Unity and Cisco CallManager. NTS offers advanced TTY features for business and individual use.



## Integrating a Fax Server with Cisco Unity

### Overview: Fax Server Integration

Integrating a fax server with Cisco Unity allows subscribers to manage their fax messages as follows:

- Subscribers can hear new fax messages announced with other messages when they call and log on to Cisco Unity. During message playback for a fax message, subscribers hear the message summary and any voice annotation but not the contents of the fax message.
- Subscribers can forward a fax message to another subscriber, or reply with a voice message if the fax message is from another subscriber, with the following limitation:



#### Caution

Do not record an introduction or add any attachments to the body of a forwarded fax message, or the Lotus Domino server resets the message type to e-mail. This causes Cisco Unity to be unable to recognize the forwarded message as a fax. Therefore, the message does not appear in the fax message count, the fax message notification will not work, and the fax phone conversation will not present the option to forward the message to a fax machine. Subscribers can view forwarded fax messages with attachments and/or with voice introductions only by using the Lotus Notes client.

- Subscribers can receive notification of new fax messages, along with other types of messages, by phone or pager.
- Subscribers can have their fax messages delivered to a fax machine. If there are attachments to a fax message, Cisco Unity renders only those attachments with the file extensions specified during setup. Other types of attachments are removed, and Cisco Unity lists the file names at the end of the fax message.

As with other message settings, subscribers use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their fax message settings. For subscribers to have phone access to their faxes, they must be in a class of service (COS) that has the FaxMail feature selected. In addition, those subscribers who will have their e-mail messages delivered to a fax machine must be in a COS that has the Text to Speech feature selected.

See the following sections in this chapter for more information:

- [Fax Server Integration, page 12-2](#)—This section describes how Cisco Unity and the fax server communicate, how the fax server routes inbound and outbound fax messages, and how subscribers view and address fax messages from their e-mail clients.
- [Task List: Integrating a Fax Server, page 12-3](#)—This section outlines the setup steps for integrating a fax server with Cisco Unity.

## Fax Server Integration

Cisco Unity supports fax servers that can install a Lotus Domino/Notes gateway and have dedicated fax lines set up to the fax ports on the fax server. A list of officially supported fax servers that you can use with Cisco Unity can be found in *Cisco Unity System Requirements, and Supported Hardware and Software*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).

Cisco Unity communicates with Lotus Domino to access and send fax messages, and never interacts directly with the fax server. Lotus Domino and the fax gateway, if used by the fax server, provide the means for Cisco Unity and the fax server to communicate. If utilized, a fax gateway is registered with Lotus Domino to handle any message that includes FAX at the beginning of the message address. The gateway transfers outgoing fax messages from Lotus Domino to the fax server and converts the messages to a format that the fax server recognizes. Similarly, the gateway transfers and converts incoming fax messages.

Cisco Unity recognizes faxes in a subscriber mailbox by the origin or destination domain name. All fax servers that support Lotus Domino use a special domain name to which all faxes are routed, for example, Name@Company@FaxDomain. You identify the domain name that you want Cisco Unity to recognize during setup.

When a subscriber who has called and logged on to Cisco Unity wants a fax or e-mail message delivered to a fax machine, Cisco Unity sends the message to Lotus Domino by using the domain address defined during setup, for example, Name@FaxDomain. The fax gateway (if present) then forwards the message to the fax server. The fax server faxes the message through a fax port.

If attachments are included with a fax or an e-mail message sent to a fax machine, Cisco Unity sends only those attachments that match the list of file name extensions that were selected during setup. Most fax products support .dcx, .tif, and .txt files, and you can add other file extensions as needed that are supported by your fax gateway and fax server. If an attachment cannot be sent to the fax machine, the file name is printed at the bottom of the message.

## Fax Server Administration

The fax server, not Cisco Unity, is responsible for routing inbound fax messages to a subscriber mailbox, and for managing and logging inbound and outbound fax messages. Additional functionality such as generating reports, and providing cover pages and least-cost routing are controlled by the fax server, not Cisco Unity. The Cisco Unity Administrator is not used in any way to administer the fax server or the services provided by the fax server.

## Sending and Receiving Faxes with an E-Mail Client

The way in which subscribers view the contents of fax messages from their computers depends on the fax server program. For example, some programs display icons to distinguish fax messages from regular e-mail messages, and they may provide a viewer to display the contents of fax messages. Alternatively, in other programs, fax messages may appear in e-mail messages as attached .tif files, which subscribers can open in a TIF viewer.

The way in which subscribers address fax messages they send from their computers also depends on the fax program. For example, some programs make it easy for subscribers to use the correct address format by providing a form on which to enter the recipient name and fax phone number.

Cisco Unity and Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity play no role in how subscribers send or receive fax messages from their computers.

## Task List: Integrating a Fax Server

If you already have a fax server installed and set up, skip the tasks below that do not apply.

1. Install the fax server by using the fax server manufacturer documentation.  
The fax server software, fax cards (if used), and fax lines must be installed on the fax server, not on the Cisco Unity server.
2. Set up inbound fax routing. See the [“To Set Up Inbound Fax Routing”](#) section on page 12-3.
3. In the Cisco Unity Administrator, enter Restriction Table settings.  
Modify the Default Fax Restriction Table, or create a new one, as needed. See the [“Creating and Modifying Restriction Tables”](#) section on page 25-3 for more information.
4. In the Cisco Unity Administrator, enter Class of Service Feature settings.  
Set FaxMail for those subscribers who access fax messages. Set both FaxMail and Text to Speech e-mail for those subscribers who want e-mail messages delivered to a fax machine. Also specify the restriction table used to control the phone numbers subscribers can use for fax delivery. Depending on how Cisco Unity subscriber accounts are set up, you may want to create a new class of service (COS) with one or both of these features, then reassign subscribers to the COS as applicable. See the [“Class of Service Features Settings”](#) section on page 14-9 for more information.
5. Test fax inbound routing to a subscriber.  
Send a fax from a fax machine to the fax server and confirm that the fax message gets routed to the mailbox of the intended recipient.

### To Set Up Inbound Fax Routing

- 
- Step 1** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
  - Step 2** In the left pane of the Tools Depot window, under Administrative Tools, double-click **Third Party Fax Administration**.
  - Step 3** Enter your fax domain, and confirm the file extensions allowed. Add other file extensions supported by the fax gateway if needed.
  - Step 4** Click Apply.
  - Step 5** Restart the Cisco Unity server for the changes to take effect.
-





## Subscriber Template Settings

### Overview: Subscriber Template Settings

When you create subscriber accounts in Cisco Unity, you can base each account on a subscriber template. Subscriber templates contain settings that are applicable for most subscribers of a particular type (such as a department).

Basing new subscriber accounts on a template minimizes the number of settings that must be modified on individual subscriber accounts, making the job of creating subscribers easier. It is important to note that changes to settings in a template do not affect any existing subscriber accounts that were based on that template. Once you create subscribers, you cannot use a template to modify them. Instead, you can:

- Customize subscriber settings for individual accounts in the Cisco Unity Administrator (see the “[Subscriber Settings](#)” chapter for details).
- Use the Bulk Edit utility to modify a subscriber setting shared by multiple subscriber accounts. For example, you might use this tool to change a setting so that a group of subscribers will no longer be listed in the phone directory, or you can associate a group of subscribers with a particular class of service. Bulk Edit is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop.)
- (Re)run the Cisco Unity Bulk Import wizard when you want to modify unique subscriber settings—such as phone passwords or extensions—for multiple subscribers at once. To do so, refer to the Cisco Unity Bulk Import wizard online Help. (To access the Cisco Unity Bulk Import wizard, on the Windows Start menu, click Programs > Cisco Unity > Cisco Unity Bulk Import.)

Note that subscribers can also customize some of their own settings either by accessing the Cisco Unity Assistant or by using the subscriber phone conversation. (In version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

### Predefined Templates

Cisco Unity comes with the following predefined subscriber templates:

- {Default Subscriber} Template—The settings on this template are suitable for most subscribers.
- {Default Administrator} Template—The Class of Service setting on this template assigns subscribers to the {Default Administrator} class of service, which gives subscribers access to the Cisco Unity Administrator.

See the following sections in this chapter for more information:

- [Creating and Modifying Templates, page 13-2](#)

- [Subscriber Template Profile Settings, page 13-2](#)
- [Subscriber Template Account Settings, page 13-4](#)
- [Subscriber Template Passwords Settings, page 13-4](#)
- [Subscriber Template Conversation Settings, page 13-5](#)
- [Subscriber Template Call Transfer Settings, page 13-9](#)
- [Subscriber Template Greetings Settings, page 13-11](#)
- [Subscriber Template Caller Input Settings, page 13-13](#)
- [Subscriber Template Messages Settings, page 13-15](#)
- [Subscriber Template Distribution Lists Settings, page 13-17](#)
- [Subscriber Template Message Notification Settings, page 13-17](#)

## Creating and Modifying Templates

You can modify the predefined templates, but you cannot delete them. You can also create an unlimited number of additional templates.

### To Create a New Template

---

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Template** page.
  - Step 2** Click the **Add** icon.
  - Step 3** In the Add a Subscriber Template dialog box, enter a name.
  - Step 4** Select **New Template** or **Based on Existing Template**. If you select Based on Existing Template, select the applicable template in the Based On field.
  - Step 5** Click the **Add** button.
  - Step 6** Enter settings for your new template, and then click the **Save** icon.
- 

### To Modify a Template

---

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Template** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Double-click the template that you want to modify.
  - Step 4** Change settings as applicable, and then click the **Save** icon.
- 

## Subscriber Template Profile Settings

Profile settings define how Cisco Unity identifies a subscriber. Some of these settings are defined in the subscriber template, but most are defined in the Cisco Unity account for each individual subscriber.

Use the following table to learn more about subscriber template profile settings.

**Table 13-1** *Subscribers > Subscriber Template > Profile Page*

Field	Considerations
Name	This displays the name of the template. To change the name of the template, enter a new name here, and then click the Save icon.
Class of Service	Select the class of service to which subscribers are assigned. The class of service defines permissions and restrictions for using Cisco Unity. To view the details of the selected class of service, click the View link. Note that when you click the link, you leave the Subscribers > Subscriber Template > Profile page, and move to the Subscribers > Class of Service > Profile page.
Active Schedule	Select a schedule to specify the days and times that the standard and closed subscriber greetings play, as well as the action that Cisco Unity takes after the greeting. To view details of the selected schedule, click the View link. Note that when you click the link, you leave the Profile page, and move to the System > Schedules page.
Time Zones	<p>Select the desired time zone for the subscriber. The default time zone setting is Default, which is the time zone set on the Cisco Unity server. Change this setting only for those subscribers who are located in a different time zone than the Cisco Unity server. The subscriber time zone setting is used for:</p> <ul style="list-style-type: none"> <li>• The Message Received Time—When a subscriber listens to messages over the phone, Cisco Unity announces the time that a message was received by using the local time specified for the subscriber.</li> <li>• The Message Notification Schedule—The schedule displayed on the subscriber Message Notification page and in the Cisco Unity Assistant uses the local time specified for the subscriber.</li> </ul> <p>Note that even if you change the time zone setting for a subscriber, the time zone setting on the Cisco Unity server is used to determine when standard and closed greetings are played for callers.</p>
Switch <i>(for dual phone system integrations only)</i>	<p>Select the phone system that the subscriber uses. If this setting is incorrect, Cisco Unity will not be able to:</p> <ul style="list-style-type: none"> <li>• Transfer calls to or from the subscriber.</li> <li>• Turn message waiting indicators (MWIs) on or off.</li> <li>• Dial the subscriber extension when the phone is selected as the recording and playback device for the Media Master.</li> </ul> <p>On the System &gt; Ports page, the selected phone system must have an appropriate number of ports set to answer calls and to dial out for MWIs and Media Master recording and playback by phone.</p>
Display Name Generation	<p>Select the format for displaying the names of new subscribers.</p> <p>Choose either First Name Then Last Name (Jessie Smith) or Last Name Then First Name (Smith, Jessie).</p> <p>If your organization uses a format other than those listed, you must select one of these options anyway, then manually adjust the display name in each subscriber account.</p>

**Table 13-1** *Subscribers > Subscriber Template > Profile Page (continued)*

Field	Considerations
Set Subscriber for Self-Enrollment at Next Login	<p>Check this check box so that the subscriber will be asked at the next logon to record a name and a standard greeting, to set a password, and to choose whether to be listed in directory assistance.</p> <p>Once the subscriber has enrolled, the check box is unchecked automatically. This setting is most commonly used for new subscribers.</p>
List in Phone Directory	<p>Check this check box to list the subscriber in directory assistance, which callers can use to reach subscribers. In addition to checking this check box, note that subscribers must also have recorded names to be listed in the phone directory.</p> <p>When allowed by the class of service, subscribers can change this setting over the phone or by using the Cisco Unity Assistant.</p>

## Subscriber Template Account Settings

You can use account settings to lock all subscriber accounts and to provide a billing ID.

Use the following table to learn more about subscriber template account settings.

**Table 13-2** *Subscribers > Subscriber Template > Account Page*

Field	Considerations
Cisco Unity Account Status	<p>Check this check box to lock subscriber accounts that are associated with this template; uncheck it to unlock the account(s).</p> <p>When an account is locked, subscribers associated with this template cannot access Cisco Unity account by phone, but they can access it by using the Cisco Unity Administrator, the Cisco Personal Communications Assistant (PCA), and Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.</p>
Billing ID	Enter organization-specific information, such as accounting information, department names, or project codes. This information can be included in subscriber reports.

## Subscriber Template Passwords Settings

The password settings on the Subscribers > Subscriber Template > Passwords page govern how subscribers initially log on to Cisco Unity by phone. The default phone password is 12345. The password settings also define whether subscribers set their own phone passwords and when they must change their passwords.

To protect Cisco Unity from unauthorized access, the default phone password should be changed. You can change the default phone password on the subscriber template before you use it to create subscriber accounts. Alternatively, you can use the Cisco Unity Bulk Import wizard to change the phone passwords for multiple subscribers at the same time after you create them. (Refer to the Cisco Unity Bulk Import online Help for details.)

As a best practice, specify a long—eight or more digits—and non-trivial password when you set subscriber passwords, and if you allow subscribers to change their own passwords, encourage them to do the same. See the [“Phone Password Restriction Settings”](#) section on page 19-1 for information on

specifying the minimum length for phone passwords, and the other ways in which you can secure phone access, such as specifying that Cisco Unity check for trivial passwords, prohibit the use of blank phone passwords and passwords that never expire, and maintain a record of previously used passwords.

The password for accessing the Cisco Unity Administrator and the Cisco PCA is inherited from the password settings in Domino and Windows (if the subscriber has a Windows domain account). However, for increased security, you can prohibit the use of blank passwords, even when the Domino or Windows account allows them. (See the [“Authentication Settings”](#) section on page 28-11 for details.)

Note that subscribers cannot use the Cisco Unity phone conversation or the Cisco Unity Assistant to change their Cisco Unity Administrator or Cisco PCA passwords, nor can administrators change them in the Cisco Unity Administrator.

Use the following table to learn more about subscriber template passwords settings.

**Table 13-3** *Subscribers > Subscriber Template > Passwords Page*

Field	Considerations
User Cannot Change Password	<p>Check this check box to prevent the subscriber from changing the phone password. Use of this setting is most applicable for accounts that can be accessed by more than one person. When you check this check box, also check the Password Never Expires check box.</p> <p>If you leave this check box unchecked, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Encourage them to specify long—eight or more digits—and non-trivial passwords as a way to protect their accounts from unauthorized access. (The minimum phone password length is specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page).</p>
User Must Change Password at Next Login	<p>Check this check box when you have set a temporary phone password, and want the subscriber to set a new password the next time that the subscriber logs on to Cisco Unity by phone.</p> <p>Encourage subscribers to specify long—eight or more digits—and non-trivial passwords as a way of protecting their accounts from unauthorized access. (The minimum phone password length is specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page).</p>
Password Never Expires	<p>Check this check box for low-security subscribers or for accounts that can be accessed by more than one person.</p> <p>Uncheck the check box to require the subscriber to change the phone password at the interval specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page.</p>
Phone Password for New Subscribers	<p>Enter a password by using digits 0 through 9. To protect Cisco Unity from unauthorized access, enter a long—eight or more digits—and non-trivial password. (The minimum length of the password is set on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page.)</p> <p>All new subscriber accounts that will be based on this template will be assigned this password when added. To have Cisco Unity prompt subscribers to set a new password, also check the User Must Change Password at Next Login check box.</p>
Last Phone Password Change	<i>Display only.</i> This setting shows the date that the password was last changed.

## Subscriber Template Conversation Settings

The Cisco Unity conversation—or the TUI (telephone user interface)—is a set of prerecorded instructions and options that Cisco Unity plays over the phone to subscribers when they listen to, send, and manage messages, and when they change their Cisco Unity settings. Conversation settings define some of what subscribers hear and how they hear it.

Some of the customizations that you can make by using the conversation settings include:

- Setting volume level, and selecting the language in which Cisco Unity plays instructions to the subscriber.
- Specifying which conversation style subscribers hear. You can also specify whether subscribers hear the comprehensive instructions offered by the full menus or brief menus for each conversation style. (For information on using Optional Conversation 1 rather than the standard conversation style, see the [“Activating Optional Conversation 1 for Subscribers”](#) section on page 7-3.)
- Enabling Cisco Unity to play a prompt that reminds subscribers when their alternate greeting is turned on.
- Determining whether subscribers address messages to other subscribers by entering extensions, by spelling first names, or by spelling last names.
- Dictating how messages are presented to subscribers over the phone. For example, you can specify whether subscribers hear the Message Type menu, message counts, and timestamps when they check messages, and you can specify the order in which Cisco Unity plays messages.
- Selecting the destination—such as a call handler, interview handler, subscriber, or directory assistance—that Cisco Unity sends subscribers to when they exit the subscriber conversation.

Use the following table to learn more about subscriber conversation settings. To learn more about additional ways that you and subscribers can change the conversation, see the [“How You Can Customize the Conversation”](#) section on page 7-1 and the [“How Subscribers Can Customize the Cisco Unity Conversation”](#) section on page 7-9.

**Table 13-4** *Subscribers > Subscriber Template > Conversation Page*

Field	Considerations
Menu Style	Choose one of these options: <ul style="list-style-type: none"> <li>• Full Menus—Subscribers hear comprehensive instructions; select for a new subscriber.</li> <li>• Brief Menus—Subscribers hear abbreviated versions of the full menus; select for a more experienced subscriber.</li> </ul>
Volume Level <i>(for analog or DTMF integrations only)</i>	Select the volume level at which subscribers hear the Cisco Unity conversation. Subscribers can also adjust the volume temporarily from their phones.
Language	Select the language in which the subscriber conversation plays instructions to subscribers.  The language setting also controls the language used for Text to Speech (TTS). (Note that to use TTS, your organization must purchase TTS licenses and install the applicable TTS languages. TTS is controlled by class of service.)  The TTY language allows TTY subscribers to read Cisco Unity prompts and to record messages by using a TTY device. TTY functionality is supported only when G.711 is selected as the system-wide message recording and storage codec.

Table 13-4 Subscribers &gt; Subscriber Template &gt; Conversation Page (continued)

Field	Considerations
Time Format	<p>Select the time format used for the message timestamps that subscribers hear when they listen to their messages over the phone:</p> <ul style="list-style-type: none"> <li>• System Default—Subscribers hear message timestamps in the time format specified in the Use 24-Hour Time Format for Conversation and Schedules field on the System &gt; Configuration &gt; Settings page.</li> <li>• 12-Hour Clock—Subscribers hear 1:00 PM when listening to the timestamp for a message left at 1:00 PM.</li> <li>• 24-Hour Clock—Subscribers hear 13:00 when listening to the timestamp for a message left at 1:00 PM.</li> </ul> <p>Subscribers can set their own time format preferences in the Cisco Unity Assistant.</p>
Conversation Style	<p>Select the conversation style that subscribers hear when they listen to and manage their messages over the phone:</p> <ul style="list-style-type: none"> <li>• Standard Conversation—Subscribers hear the menus depicted in the <i>Cisco Unity Phone Menus for the Standard Conversation</i>.</li> <li>• Optional Conversation 1—Subscribers hear the menus depicted in the <i>Cisco Unity Phone Menus for Optional Conversation 1</i>.</li> </ul> <p>You can use either full or brief menu style with each conversation style.</p>
When Exiting the Conversation, Send Subscriber To	<p>Select the destination to which Cisco Unity sends the subscriber when exiting the conversation.</p> <ul style="list-style-type: none"> <li>• Call Handler—Sends the call to the call handler that you select.</li> <li>• Directory Handler—Sends the call to directory assistance.</li> <li>• Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>• Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>• Interview Handler—Sends the call to the interview handler that you select.</li> <li>• CVM Mailbox Reset—Sends the call to the mailbox reset conversation. (Available only when you use the Community Voice Mail package.)</li> <li>• Sign-In—Sends the call to the subscriber logon conversation.</li> <li>• Subscriber—Sends the call to the subscriber that you select.</li> </ul>
Identify a Subscriber By	<p>Select how the conversation prompts subscribers to address messages to other subscribers. Subscribers can address messages over the phone by entering subscriber extensions, by spelling their first names, or by spelling their last names. Addressing by name requires lettered keypads on subscriber phones.</p> <p>Regardless of the option you choose here, as subscribers address a message by phone, they can switch between addressing by name and addressing by extension by pressing the # key twice. However, when the Enable Spelled Name Search check box is unchecked on the System &gt; Configuration &gt; Settings page, subscribers can address messages over the phone only by entering subscriber extensions.</p>
Subscriber Recorded Name	<p>Check this check box to have Cisco Unity play the recorded name of the subscriber when the subscriber accesses Cisco Unity by phone.</p> <p>Uncheck the check box to have Cisco Unity go directly to the message count.</p>

Table 13-4 Subscribers &gt; Subscriber Template &gt; Conversation Page (continued)

Field	Considerations
Alternate Greeting Notification	<p>Check this check box to have Cisco Unity notify subscribers when they have their alternate greeting turned on.</p> <p>Cisco Unity plays the notification immediately after subscribers log on to Cisco Unity by phone, and then Cisco Unity plays a menu from which subscribers can choose to leave their alternate greeting on, turn it off, or play it.</p>
Message Count Totals	Check this check box to have Cisco Unity announce the total number of messages that are marked new. The number includes voice, e-mail, fax, and receipt messages, as applicable.
Voice Message Count	Check this check box to have Cisco Unity announce the number of voice messages that are marked new.
E-Mail Message Count	Check this check box to have Cisco Unity announce the number of e-mail messages that are marked new.
Fax Count	Check this check box to have Cisco Unity announce the number of fax messages that are marked new.
Saved Message Count	Check this check box to have Cisco Unity announce the total number of messages that have been saved. The number includes voice, e-mail, fax, and receipt messages.
Message Type Menu	<p>Check this check box so that Cisco Unity plays the following menu when subscribers log on to Cisco Unity over the phone:</p> <ul style="list-style-type: none"> <li>• Press 1 to hear voice messages</li> <li>• Press 2 to hear e-mails</li> <li>• Press 3 to hear faxes</li> <li>• Press 4 to hear receipts</li> </ul> <p>Note that although the e-mail and fax options are available in the Message Type Menu, Cisco Unity plays e-mails and faxes only when the subscriber is assigned to a class of service that has the Text to Speech (TTS) and FaxMail features enabled. With fax messages, Cisco Unity plays only message properties (for example, the sender, date, and time).</p> <p>Subscribers can also enable the Message Type menu by using the Cisco Unity Assistant.</p>
Sort by Message Type	<p>Select a message type, and then click the Move Up and Move Down buttons to reorder the list of message types. Cisco Unity plays messages in the order that you specify here.</p> <p>Cisco Unity plays e-mails and faxes only when the subscriber is assigned to a class of service that has the Text to Speech (TTS) and FaxMail features enabled. With fax messages, Cisco Unity plays only message properties (for example, the sender, date, and time).</p> <p>Subscribers can also specify the order in which Cisco Unity plays new and saved messages by using the Cisco Unity Assistant.</p>
Then By	<p>Click Newest First or Oldest First to specify the message order for new and saved messages.</p> <p>Note that except for receipts, urgent messages are always played before regular messages for each message type (receipts are sorted by the time that they were sent).</p>

**Table 13-4** *Subscribers > Subscriber Template > Conversation Page (continued)*

Field	Considerations
Sender's Information	<p>Check this check box so that Cisco Unity plays caller information about a message sender before playing a message. The information that Cisco Unity plays depends on how Cisco Unity is set up.</p> <p>By default, Cisco Unity plays the following information when the Sender's Information check box is checked:</p> <ul style="list-style-type: none"> <li>For messages left by an identified subscriber, Cisco Unity plays the recorded name of the subscriber before playing the message. If the subscriber does not have a recorded name, Cisco Unity plays the primary extension associated with the subscriber instead.</li> <li>For messages left by an unidentified caller, Cisco Unity does not provide the phone number (ANI or caller ID) information before playing the message.</li> </ul> <p>However, you can use the Bulk Edit utility (available in Tools Depot) to enable Cisco Unity to announce additional caller information when the Sender's Information check box is checked:</p> <ul style="list-style-type: none"> <li>For messages left by an identified subscriber, Cisco Unity plays the recorded name (if available) and the extension before playing the message.</li> <li>For messages left by unidentified caller, Cisco Unity plays the phone number (if available) of the caller before playing the message.</li> </ul>
Message Number	<p>Check this check box to have Cisco Unity announce the sequential number of a message ("Message one...").</p> <p>Use with the Message Count Totals check box to help subscribers keep track of the number of unheard messages.</p>
Before Playing Each Message, Play: Time the Message Was Sent	<p>Check this check box to have Cisco Unity announce the date and time a message was sent, before playing the message.</p>
After Playing Each Message, Play: Time the Message Was Sent	<p>Check this check box to have Cisco Unity announce the date and time a message was sent, after playing the message.</p>

## Subscriber Template Call Transfer Settings

Call transfer settings specify whether unidentified callers are transferred to a phone or to the greetings of a subscriber or handler. These settings also specify how Cisco Unity handles a transfer: Cisco Unity can either release the call to the phone system, or it can supervise the transfer.

When Cisco Unity is set to supervise transfers, it can provide additional call control with call holding and call screening:

- With call holding, when the phone is busy, Cisco Unity can ask callers to hold. Cisco Unity plays hold music, and approximately every 30 seconds, tells callers on hold how many callers are ahead of them and allows them to continue holding, leave a message, or try another extension. There is no limit to the number of callers that can be holding.

If call holding is not selected, callers are sent to whichever subscriber or handler greeting is enabled—either the busy, standard, closed, or alternate greeting.

- With call screening, Cisco Unity can ask for the name of the caller before connecting to a subscriber. The subscriber can then hear who is calling and, when a phone is shared by more than one subscriber, who the call is for. The subscriber can then accept or refuse the call.

If the call is accepted, it is transferred to the subscriber phone. If the call is refused, Cisco Unity plays the applicable subscriber greeting.

Use the following table to learn more about subscriber template call transfer settings.

**Table 13-5** *Subscribers > Subscriber Template > Call Transfer Page*

Field	Considerations
Transfer Incoming Calls to Subscriber's Phone	<p>Choose one of these options:</p> <ul style="list-style-type: none"> <li>• No (Send Directly)—The extension assigned to the subscriber does not ring for unidentified callers; Cisco Unity plays the subscriber greeting.</li> <li>• Yes, Ring Subscriber's Extension—Cisco Unity sends calls to the extension assigned to the subscriber (displayed in the adjacent box). When Supervise Transfer is selected, use in conjunction with Rings to Wait For field to set the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</li> <li>• Yes, Ring Subscriber at This Number—Cisco Unity sends calls to the number entered in the adjacent box. When Supervise Transfer is selected, use in conjunction with Rings to Wait For field to set the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</li> </ul> <p>Note that the restriction tables associated with your class of service—rather than the subscriber COS—may prohibit you from entering certain phone numbers for subscribers.</p>
Transfer Type	<p>Select how Cisco Unity transfers calls. Use this setting with caution and only if you understand its implications on the phone and voice messaging systems.</p> <ul style="list-style-type: none"> <li>• Release to Switch—Cisco Unity puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Cisco Unity—forwards the call to the subscriber or handler greeting. This transfer type allows Cisco Unity to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system.</li> <li>• Supervise Transfer—Cisco Unity acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Cisco Unity—not the phone system—forwards the call to the subscriber or handler greeting. You can use supervised transfer whether or not the phone system forwards calls.</li> </ul> <p>The Transfer Type option is unavailable when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Rings to Wait For	<p>Select the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</p> <p>Set this value to at least 3 to give subscribers a chance to answer. Avoid setting to more than 4, especially if the call may be transferred to another extension, where the caller might have to wait for another four rings. This value should be at least two rings fewer than the phone system setting for forwarding calls.</p> <p>This option is unavailable when Transfer Incoming Calls is set to the No (Send Directly) option and when Release to Switch is selected.</p>

Table 13-5 Subscribers &gt; Subscriber Template &gt; Call Transfer Page (continued)

Field	Considerations
If the Call Is Busy	<p>Select the action that Cisco Unity performs for unidentified callers when the subscriber phone is busy. You may want to use holding options sparingly, because having calls on hold can tie up ports.</p> <ul style="list-style-type: none"> <li>• Always Hold—Cisco Unity plays a prompt indicating that the extension is busy. The caller is put on hold.</li> <li>• No Holding—Cisco Unity prompts the caller to leave a message and allows the caller to dial another extension.</li> <li>• Ask Caller—Cisco Unity gives the caller the options of holding, leaving a message, or dialing another extension.</li> </ul> <p>These options are unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Announce	<p>Check this check box to have Cisco Unity say “transferring call” when the subscriber answers the phone, to indicate that the call is from an unidentified caller.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Introduce (Call for Name)	<p>Check this check box to have Cisco Unity say “call for &lt;subscriber recorded name&gt;” or “call for &lt;dialled extension number&gt;” when the subscriber answers the phone. This setting applies only to calls from unidentified callers. Use this setting when subscribers share a phone or a subscriber takes calls from more than one dialed extension.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Confirm (Call Can Be Accepted or Refused)	<p>Check this check box to have Cisco Unity prompt the subscriber to accept or refuse a call from an unidentified caller. If the call is accepted, it is transferred to the subscriber phone. If the call is refused, Cisco Unity plays the applicable subscriber greeting. You use this setting with the Ask Caller’s Name setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Ask Caller’s Name	<p>Check this check box to have Cisco Unity prompt unidentified callers to say their names. When the phone is answered, the subscriber hears “Call from...” before Cisco Unity transfers the call. You use this setting with the Confirm setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>

## Subscriber Template Greetings Settings

Each subscriber and call handler can have up to five greetings. The greeting settings specify which greetings are enabled and the actions that Cisco Unity takes during and after each greeting. Enabling a greeting makes it available for Cisco Unity to use in appropriate situations.

The greeting that plays when a caller reaches a subscriber or call handler depends on:

- The active schedule.
- The greeting source.
- Whether the call is internal.

- Whether the called extension is busy.

Cisco Unity greetings for subscribers and call handlers are:

<b>Standard</b>	Plays at all times unless overridden by another greeting.
<b>Closed</b>	Plays during the closed (nonbusiness) hours defined for the active schedule. When in effect, the closed greeting overrides the standard greeting, and thus limits the standard greeting to the open hours defined for the active schedule.
<b>Internal</b>	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 and closed greetings. Not all phone system integrations provide the support necessary for an internal greeting.
<b>Busy</b>	Plays when the extension is busy. (For example, “All of our operators are with other customers.”) A busy greeting overrides the standard, closed, and internal greetings. Not all phone system integrations provide the support necessary for a busy greeting.
<b>Alternate</b>	<p>Can be used for a variety of special situations, such as vacations or a holiday. (For example, “I will be out of the office until...”)</p> <p>Neither you nor Cisco Unity subscribers can schedule in advance when or for how long an alternate greeting is enabled. When enabled, an alternate greeting plays until you or the subscriber disables it, and overrides all other greetings.</p> <p>You can enable Cisco Unity to notify subscribers when their alternate greeting is turned on, by changing a setting on the template and subscriber Conversation pages in the Cisco Unity Administrator.</p>

Subscribers can manage all of their greetings by phone, or by using the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

Use the following table to learn more about subscriber template greeting settings.

**Table 13-6** *Subscribers > Subscriber Template > Greetings Page*

<b>Field</b>	<b>Considerations</b>
Greeting	Select the greeting that you want to specify settings for. This setting does not reflect which of the greetings is active.
Status	Indicate whether the selected greeting is enabled. When a greeting is enabled, Cisco Unity plays it in the applicable situation. Recording a greeting does not automatically enable it; it must be enabled here.
Source	<p>Indicate the source for the greeting selected in the Greeting field:</p> <ul style="list-style-type: none"> <li>• <b>System</b>—Select to use the prerecorded system default greeting. Cisco Unity plays a prerecorded greeting along with the recorded name of the subscriber (for example, “Sorry, &lt;subscriber name&gt; is not available”). If the subscriber does not have a recorded name, Cisco Unity plays the subscriber extension instead.</li> <li>• <b>Recording</b>—Select to use a personal recording for the subscriber (or call handler). To record and play greetings here, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.</li> <li>• <b>Blank</b>—Select to have no recording. When the greeting source is left blank, Cisco Unity immediately performs the after-greeting action.</li> </ul>

**Table 13-6** *Subscribers > Subscriber Template > Greetings Page (continued)*

Field	Considerations
Allow Caller Input	<p>Check this check box to enable settings specified on the Caller Input page. These settings contain actions assigned to caller key presses during the greeting. (For example, “To speak to my assistant, press 3.”)</p> <p>Click the Caller Input link to view the Caller Input page. Note that when you click the link, you leave the Greetings page.</p>
After Greeting	<p>Indicate the action that Cisco Unity performs after the greeting plays:</p> <ul style="list-style-type: none"> <li>• <b>Take Message</b>—Cisco Unity records a message from the caller. Click the Take Message link to view the Messages page.</li> <li>• <b>Say Good-Bye</b>—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• <b>Send Caller To</b>—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– <b>Call Handler</b>—Sends the call to the call handler that you select.</li> <li>– <b>Directory Handler</b>—Sends the call to directory assistance.</li> <li>– <b>Greetings Administrator</b>—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– <b>Hang Up</b>—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– <b>Interview Handler</b>—Sends the call to the interview handler that you select.</li> <li>– <b>Sign-In</b>—Sends the call to the subscriber logon conversation.</li> <li>– <b>Subscriber</b>—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>
Reprompt the User After This Many Seconds of Silence	Check this check box and enter a value in the field on the right to indicate the number of seconds of silence to allow. When Cisco Unity receives no input from a caller within this number of seconds, Cisco Unity prompts the caller again.
Number of Times to Reprompt	Indicate the number of times to reprompt a caller. After the number of times indicated here, Cisco Unity performs the after-greeting action.

## Subscriber Template Caller Input Settings

Caller input settings define actions that Cisco Unity takes in response to touchtone keys pressed by callers. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page. (See the [“Subscriber Template Greetings Settings”](#) section on page 13-11 for details.)

Caller input settings are available only in the Cisco Unity Administrator; however, the greeting that mentions the key presses can be recorded either by the subscriber or the administrator. (For example, “I am unable to take your call right now. To speak to my assistant, press 3. To leave a message, press 4. To speak to a sales representative, press 5.”)

### To Define an Action for a Key

- 
- Step 1** Select a key from the Caller Input Map or from the keypad.
- Step 2** Select an action.

**Step 3** Indicate whether to lock the key to that action.

Use the following table to learn more about subscriber template caller input settings.

**Table 13-7** *Subscribers > Subscriber Template > Caller Input Page*

Field	Considerations
Allow Callers to Dial an Extension During Greeting	<p>Check this check box to allow callers to enter an extension while the greeting plays. Use in conjunction with the Lock This Key check box to allow callers to enter some extensions but not others.</p> <p>This option is unavailable if the Allow Caller Input check box is unchecked on the Greetings page.</p>
Milliseconds to Wait for Additional Digits	<p>Indicate the amount of time Cisco Unity waits for additional input after callers press a single key that is not locked. If there is no input within this time, Cisco Unity performs the action assigned to the single key.</p> <p>A value of 1500 (one and one-half seconds) is recommended.</p> <p>This option is unavailable if the Allow Callers to Dial an Extension During Greeting check box is unchecked.</p>
Lock This Key to the Action	<p>Check this check box to have Cisco Unity ignore additional input after callers press the key; Cisco Unity performs the action assigned to the key. To create efficient caller input menus, lock all keys except those that begin extensions on your system. You also can lock a key to block calls to extensions that begin with that key.</p> <p>To lock the actions for all keys, uncheck the Allow Callers to Dial an Extension During Greeting check box.</p>

Table 13-7 Subscribers &gt; Subscriber Template &gt; Caller Input Page (continued)

Field	Considerations
Action	<p>Indicate the action that Cisco Unity performs after a caller presses the corresponding key. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page.</p> <ul style="list-style-type: none"> <li>• Ignore Key—No action taken. Cisco Unity plays the entire greeting, then performs the after-greeting action.</li> <li>• Skip Greeting—Cisco Unity skips the greeting and performs the after-greeting action. Skip Greeting is assigned to # by default to provide callers a standard way to skip greetings.</li> <li>• Take Message—Cisco Unity records a message from the caller. The greeting should indicate that a message will be recorded. Click the Take Message link to view the associated Messages page.</li> <li>• Say Good-Bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>

## Subscriber Template Messages Settings

Message settings define the following:

- The maximum recording length for messages from unidentified callers. (Note that for some integrations, you can set up Cisco Unity so that when a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. See the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19 for details.)
- What unidentified callers can do when leaving messages.
- The language of the Cisco Unity prompts that callers hear when leaving messages.
- Whether subscribers are notified that they have messages.
- The extension where the message waiting indicator (MWI) will be activated when new messages arrive.

For information on how you can change the way that Cisco Unity handles messages when calls are disconnected while subscribers are in the process of sending, replying to, or forwarding a message, see the [“How Cisco Unity Handles Messages That Are Interrupted by Disconnected Calls”](#) section on page 6-4.

Use the following table to learn more about subscriber template messages settings.

**Table 13-8** *Subscribers > Subscriber Template > Messages Page*

Field	Considerations
Maximum Message Length in Seconds	<p>Set the recording length allowed for messages left by unidentified callers. (An unidentified caller is an outside caller or a caller from inside the organization calling from a phone that is not associated with a subscriber account, such as a conference room.)</p> <p>Recipients may want to limit the length of messages from unidentified callers. Some departments, such as Customer Service, may want to permit much longer messages.</p> <p>If enabled, a warning tone will sound before the maximum message length is reached.</p>
After Message Action	<p>Indicate the action that Cisco Unity performs after an unidentified caller leaves a message:</p> <ul style="list-style-type: none"> <li>• Say Good-Bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>
Callers Can Edit Messages	<p>Check this check box to allow callers to be prompted to listen to, add to, rerecord, or delete their messages.</p> <p>Balance giving callers the additional control of editing messages with having voice messaging ports tied up for the additional time.</p>
Mark Messages as Urgent	<p>Indicate the action that Cisco Unity will allow:</p> <ul style="list-style-type: none"> <li>• Always—All messages left by unidentified callers are marked urgent. This may be useful for Sales or Technical Support call handlers.</li> <li>• Never—Messages left by unidentified calls are never marked urgent.</li> <li>• Ask Caller for Their Preference—Cisco Unity asks unidentified callers whether to mark their messages urgent.</li> </ul> <p>Note that Cisco Unity plays new urgent messages before other messages.</p>
Language That Callers Hear	<p>Select the language in which system prompts are played to callers. The language setting affects system prompts such as “You may record your message at the tone.”</p> <p>If you choose Inherited, Cisco Unity determines the language to use for system prompts on a per-call basis, depending upon the language set by the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.</p> <p>The default phone language and the list of languages shown here are set on the System &gt; Configuration &gt; Phone Languages page.</p>

**Table 13-8** *Subscribers > Subscriber Template > Messages Page (continued)*

Field	Considerations
Use MWI for Message Notification	<p>Check this check box to have Cisco Unity use the message waiting indicator (MWI) on the phone to alert the subscriber of new voice messages. MWIs are not used to indicate new e-mail, fax, or receipt messages.</p> <p>Cisco Unity uses the number listed in the table to activate a message waiting indicator (MWI). By default, the table contains an “X” to indicate the primary extension assigned to a subscriber.</p> <p>You can change this to have Cisco Unity activate MWIs for another extension or phone number on each individual subscriber page.</p>

## Subscriber Template Distribution Lists Settings

Distribution list settings allow you to specify which public distribution lists subscribers will be assigned to. For example, you might create different templates for different work groups, and create a public distribution list for each work group.

Cisco Unity automatically creates a public distribution list called All Subscribers. You may want to associate the All Subscribers list with every subscriber template.

Create the public distribution lists before setting up subscriber templates if you plan to associate public distribution lists with templates. After the subscriber accounts are created, you can add or remove subscribers from the lists on the Public Distribution Lists > Profile Page.

Use the following table to learn more about distribution list settings.

**Table 13-9** *Subscribers > Subscriber Template > Distribution Lists*

Field	Considerations
Public Distribution Lists	<p>A list of all public distribution lists that are not currently associated with the selected template.</p> <p>To assign all new subscribers based on this template to a public distribution list, select the list and click &gt;&gt;.</p>
New Subscribers Added To	<p>All public distribution lists to which new subscribers are added.</p> <p>To assign all new subscribers based on this template to a public distribution list, select the list in the Public Distribution Lists box and click &gt;&gt;.</p> <p>To remove a distribution list from those to which new subscribers are added, select the list and click &lt;&lt;.</p>

## Subscriber Template Message Notification Settings

Cisco Unity can notify a subscriber of new messages by calling a phone or pager, or by sending an e-mail. Message notification settings allow you to control how and when Cisco Unity notifies a subscriber of new messages. You can set up notification for subscribers by using the Cisco Unity Administrator, and subscribers can set it up themselves by using the Cisco Unity Assistant, if available. Subscribers can also enter the phone number and status of four of the notification devices—home phone, work phone, spare phone, and pager—in the subscriber phone conversation. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

To set up message notification, you select a notification device—phone, pager, or text pager—and enter a phone number or e-mail address, as applicable. The settings for each notification device allow you to control when and how notifications are sent to the first and subsequent devices. Generally, you adjust these settings on the message notification page of a specific subscriber and not in the subscriber template. However, you may want to enter notification settings in the subscriber template if, for example, you want to set up “chaining” or “cascading” message notification for an entire department of new subscribers. For more information, see the “[Chaining Message Notification](#)” section on page 17-21, and the “[Cascading Message Notification](#)” section on page 17-21.

Additionally, Cisco Unity can send message notifications in the form of text messages to text pagers, text-compatible cell phones, and e-mail addresses. For more information, see the “[Text Message Notifications](#)” section on page 17-22.

Use the following table to learn more about subscriber template message notification settings. To set up message notification for individual subscribers, see the “[Subscriber Message Notification Settings](#)” section on page 17-20.

**Table 13-10** *Subscribers > Subscriber Template > Message Notification Page*

Field	Considerations
Device	Select the device that you want to use for message notification.
Phone Number <i>(not available for text pager notifications)</i>	<p>Enter the phone number, including trunk access code, of the selected device. Use digits 0 through 9 and the following dialing characters in the phone number:</p> <ul style="list-style-type: none"> <li>• , (comma) to insert a one-second pause.</li> <li>• # and * to correspond to the # and * keys on the phone.</li> </ul> <p>Subscribers can change this number over the phone.</p> <p>Note that the restriction tables associated with your class of service—rather than the subscriber COS—may prohibit you from entering certain phone numbers for subscribers.</p>
Extra Digits <i>(not available for text pager notifications)</i>	Enter any extra digits that Cisco Unity will dial after the phone number. The effect of the extra digits depends on the selected device. For pagers, the extra digits are shown on the pager display.
Dialing Options <i>(not available for text pager notifications)</i>	<p>Select the dialing options:</p> <ul style="list-style-type: none"> <li>• Try to Detect Connection—Cisco Unity waits until detecting a connection to dial the digits in Extra Digits.</li> <li>• Seconds to Wait—Cisco Unity can wait a specified number of seconds before dialing the digits in Extra Digits. Use this option if the automatic call progress detection is not reliable. Examples of poor call progress detection include noisy phone lines and unusual ringing patterns.</li> </ul>
To: (E-Mail Address) <i>(available for text pager notifications only)</i>	<p>Enter the e-mail address of the subscriber text pager, text-compatible cell phone, or another e-mail account (such as a home e-mail address).</p> <p>Up to 128 characters can be entered in this field.</p>
From: (Phone Number) <i>(available for text pager notifications only)</i>	<p>Enter a phone number in this field if the subscriber has a text-compatible cell phone and wants text pager notifications to include a return phone number. Typically, this field contains the number that the subscriber calls to check messages.</p> <p>The From phone number appears in the last line of any text pager notification. A subscriber can press the Return Call button on many text-compatible cell phones to dial the phone number. The cell phone must support automatic callback in order to use this feature.</p> <p>Up to 40 characters can be entered in this field.</p>

Table 13-10 Subscribers &gt; Subscriber Template &gt; Message Notification Page (continued)

Field	Considerations
Send: <i>(for text pager notifications only)</i>	<p>Enter the text message that the subscriber wants to receive in a text pager notification. For example, you might enter “Urgent message for Technical Support” for a subscriber who is on call for the technical support department.</p> <p>Every time a message arrives that matches the criteria selected in the message notification settings, the Cisco Unity Messaging System sends this text message.</p> <p>Up to 64 characters can be entered in this field.</p>
Include Voice Mail, E-Mail, and Fax Message Counts <i>(available for text pager notifications only)</i>	<p>Check this check box if you want the text pager notification to include a count of each voice mail, e-mail, and fax message.</p> <p>When the subscriber receives the notification, the message count appears as a line for each type of message. For example:</p> <ul style="list-style-type: none"> <li>- 9 voice mail</li> <li>- 2 urgent voice mail</li> <li>- 17 urgent e-mail</li> </ul> <p>The e-mail count does not include non-delivery receipts or meeting requests.</p>
Status	<p>Indicate whether to turn message notification to this device on or off. Subscribers can change this setting over the phone.</p> <ul style="list-style-type: none"> <li>• Enabled—Cisco Unity calls the device when there are new messages.</li> <li>• Disabled—Cisco Unity does not call the device. Disabling a device does not delete its settings.</li> </ul>
Notify Subscriber Of	<p>Select the types of messages and message urgency for which Cisco Unity will call the device. If no message type is selected, Cisco Unity does not call the device.</p> <p>When setting up a chain of message notification devices, select messages in this field only for the first device. If any message types are selected for any device other than the first, message notification for this device will commence immediately and will not wait for the notification failure of the previous device. Therefore, your notifications will not chain but all trigger at once.</p>
Notification Schedule	<p>In the grid, click the blocks to change between inactive (no notifications) and active (notifications okay). Note that you can set active and inactive hours for one day, then use Copy Day’s Schedule to copy the settings to other days.</p>
Copy Day’s Schedule	<p>To avoid clicking the same blocks for more than one day, use the Copy Day’s Schedule and &gt;&gt; functions. Select a day to copy, then select which days to copy the schedule setting to.</p>
Notification Options: Send Initial Notification After How Many Minutes	<p>Specify the delay from the time a message is received until the message notification triggers (if the message matches the criteria selected in the Notify Subscriber Of section). You can space notifications on different devices at regular intervals, such as 15 minutes, to achieve a cascading message notification effect.</p> <p>If the delay time takes the notification out to a time when the device schedule is no longer active, the notification does not take place.</p> <p>The range for the delay field is 0 to 120 minutes. The default is 0 minutes.</p>

Table 13-10 Subscribers &gt; Subscriber Template &gt; Message Notification Page (continued)

Field	Considerations
Notification Options: Restart Notification or Repeat Notification	<p>Use to specify the timing of message notification according to subscriber needs. Choose one of these options:</p> <ul style="list-style-type: none"> <li>Restart Notification Each Time a New Message Arrives—When this option is selected, Cisco Unity begins a notification process immediately upon the arrival of each message that matches the selected criteria. Cisco Unity considers notification successful if the device answers, even if new messages remain. (For example, notification is considered successful even when an answering machine picks up and records the message, but the message remains unread in the e-mail Inbox.)</li> </ul> <p>Note that if you activate the Restart Notification option and the Send Initial Notification field is set to 0, then Cisco Unity triggers the message notification immediately. However, if you enter a delay in the Send Initial Notification field, then Cisco Unity delays notification that number of minutes instead of dialing immediately. Messages that arrive during the delay period will not trigger separate notifications.</p> <ul style="list-style-type: none"> <li>Repeat Notification If There Are Still New Messages After This Many Minutes—When this option is selected and a duration specified, Cisco Unity attempts notification immediately after the first message, and then initiates a notification schedule based on the specified interval. For example, if you set the repeat notification interval to 5 minutes at 11:47 AM, Cisco Unity will notify the subscriber of new messages at 11:50 AM, 11:55 AM, 12:00 PM, 12:05 PM, 12:10 PM, 12:15 PM, 12:20 PM, 12:25 PM, and so on. The notification schedule is effective for as long as the subscriber has one or more new messages.</li> </ul> <p>The range for the redial frequency field is 1 to 100 minutes.</p>
If Device Does Not Answer <i>(not available for text pager notifications)</i>	<p>Indicate settings for the following:</p> <ul style="list-style-type: none"> <li>Wait for How Many Rings Before Hanging Up—Set to a minimum of 3 rings. Choose a higher number to give a subscriber more time to get to the phone.</li> <li>Try Again How Many Times—Choose a higher number to reach a subscriber who steps away from the phone briefly. Choose a lower number to avoid disturbing others.</li> <li>How Many Minutes to Wait Between Tries—Choose a higher number to reach a subscriber who is away from the phone for long periods of time.</li> </ul>
If Device Is Busy <i>(not available for text pager notifications)</i>	<p>Indicate settings for the following:</p> <ul style="list-style-type: none"> <li>Try Again How Many Times—Choose a higher number to reach a subscriber who uses the phone frequently.</li> <li>How Many Minutes to Wait Between Tries—Choose a higher number to reach a subscriber who has long phone conversations.</li> </ul>
If Notification Fails, Send Notification To <i>(not available for text pager notifications)</i>	<p>Select an option for an additional device to send notification to when the first device does not answer or is busy, and the maximum number of retries has been reached. Cisco Unity calls the next device only if it is enabled and its schedule is current.</p> <p>Cisco Unity considers message notification successful if a device answers, even if, for example, an answering machine answers. Cisco Unity considers that message notification has failed only after all selected no-answer and busy signal retries have been exhausted.</p>

**Table 13-10 Subscribers > Subscriber Template > Message Notification Page (continued)**

<b>Field</b>	<b>Considerations</b>
Switch <i>(for dual phone system integrations only)</i>	Select the phone system that Cisco Unity dials out on when notifying the subscriber of new messages. Each notification device (except for text pagers) can be associated with a specific phone system.  On the System > Ports page, the selected phone system must have at least one port set to dial out for message notification.





## Class of Service Settings

### Overview: Class of Service Settings

A class of service (COS) defines limits and permissions for using Cisco Unity. For example, a COS:

- Controls access to the Cisco Unity Administrator and to features, such as Text to Speech e-mail or live reply.
- Controls how subscribers interact with Cisco Unity. For example, a COS dictates the maximum length of subscriber messages and greetings, whether subscribers can choose to be listed in directory assistance, and whether subscribers can send messages to a public distribution list.
- Specifies the restriction table used to control the phone numbers subscribers can use for fax delivery, message notification, call transfer, and other tasks.

A COS is specified in each subscriber template; thus, a subscriber is assigned to the COS which is specified in the template upon which the subscriber account is based.

### Predefined Classes of Service

Cisco Unity includes the following predefined classes of service, which you can modify but not delete.

<b>{Default Subscriber}</b>	Contains settings that are applicable to subscribers. By default, this COS is associated with the {Default Subscriber} template.
<b>{Default Administrator}</b>	Contains settings that are applicable to Cisco Unity administrators. By default, this COS has all the settings checked on the Subscribers > Class of Service > System Access Page.

See the following sections in this chapter for more information:

- [How a Class of Service Works, page 14-2](#)
- [Creating and Modifying Classes of Service, page 14-2](#)
- [Class of Service Profile Settings, page 14-3](#)
- [Class of Service Subscriber Settings, page 14-4](#)
- [Class of Service System Access Settings, page 14-5](#)
- [Class of Service Call Transfer Settings, page 14-8](#)
- [Class of Service Messages Settings, page 14-8](#)

- [Class of Service Greetings Settings, page 14-9](#)
- [Class of Service Features Settings, page 14-9](#)
- [Class of Service Restriction Table Settings, page 14-10](#)

## How a Class of Service Works

A COS is specified in each subscriber template, and controls what subscribers can do in Cisco Unity. This means that when a subscriber wants to update call transfer settings, for example, the COS that is associated with the subscriber's account determines whether the subscriber can make the desired change. This is true whether the subscriber is logged onto Cisco Unity by phone, or is using the Cisco Unity Assistant.

On the other hand, when an administrator uses the Cisco Unity Administrator to change settings for the subscriber, Cisco Unity does not consider the limitations set by the subscriber COS. Instead, Cisco Unity considers the limitations set by the administrator COS before permitting the change. This allows an administrator, when necessary, to override the limitations of the COS of a particular subscriber.

## Creating and Modifying Classes of Service

You can modify the predefined classes of service, and you can create new ones by using the following procedures. Changes to the settings in a COS affect not only new members, but also existing members of the COS. COS settings cannot be changed in individual subscriber Cisco Unity accounts; however, a subscriber can be reassigned to a different COS at any time.

When a COS includes access to a feature that requires individual licenses, you can assign groups of subscribers to the COS only if enough licenses are available.

Note that you cannot delete a COS that has subscribers assigned to it without first reassigning the subscribers to another COS. To do so, see the last procedure in the [“To Assign or Reassign Subscribers to a Class of Service”](#) section on page 14-3.



### Caution

If you do not have at least one Windows domain account with membership in a COS that offers access to the Cisco Unity Administrator, you may lose the ability to administer Cisco Unity, and be required to reinstall. As a best practice, make sure that at least one account is associated with a subscriber account assigned to the Default Administrator COS.

### To Create a New Class of Service

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Class of Service dialog box, enter information as applicable in the Name field.
- Step 4** Select **New Class of Service** or **Based on Existing Class of Service**. If you select Based on Existing Class of Service, select the applicable class of service in the Based On field.
- Step 5** Click the **Add** button.
- Step 6** Enter settings for your new class of service, and then click the **Save** icon.

### To Modify a Class of Service

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Double-click the COS that you want to modify.
  - Step 4** Change settings as applicable, and then click the **Save** icon.
- 

### To Assign or Reassign Subscribers to a Class of Service

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Double-click the name of the class of service to which subscribers are currently assigned.
  - Step 4** Go to the **Subscribers > Class of Service > Subscribers** page.
  - Step 5** Click **Assign** or **Reassign**, as applicable.
  - Step 6** Enter the name of a subscriber. You also can enter \* for a list of all subscribers, or enter one or more characters followed by \* to narrow your search.
  - Step 7** Click **Find**.
  - Step 8** From the list provided, select the names of the subscribers to be assigned or reassigned. To select more than one name, hold down the Ctrl or Shift key.
  - Step 9** Do one of the following actions, as applicable:
    - Click the **Assign** button.
    - Select the applicable class of service, and then click the **Reassign** button.
- 

## Class of Service Profile Settings

Class of service profile settings specify whether subscribers can record their own voice names and change their directory listing status. You can also indicate whether subscribers assigned to a class of service use regular or enhanced phone security. For details on setting up enhanced phone security, see the “[Enhanced Phone Security](#)” chapter.

Use the following table to learn more about COS profile settings.

**Table 14-1** *Subscribers > Class of Service > Profile Page*

Field	Considerations
Name	<i>Display only.</i> This setting shows the name of the COS.
Subscribers Can Record Their Own Voice Name	Uncheck the check box to prevent subscribers assigned to this COS from recording their own names (for example, if your organization has all names and greetings recorded in one voice).
Maximum Recorded Name Length in Seconds	Indicate the number of seconds after which Cisco Unity stops recording the name of a subscriber assigned to this COS.

Table 14-1 *Subscribers > Class of Service > Profile Page (continued)*

Field	Considerations
Listing Subscribers in the Phone Directory	<p>Indicate whether subscribers assigned to this COS can choose to be listed in directory assistance.</p> <p>Directory assistance is the audio listing that subscribers and unidentified callers use to reach subscribers and to leave messages.</p>
Phone Security	<p>Indicate whether subscribers assigned to this COS use regular or enhanced phone security. Regular security requires subscribers to use passwords when logging on to Cisco Unity. Enhanced security adds RSA two-factor user authentication to regular security.</p> <p>Note that this field is available only when RSA Two Factor is checked on the System &gt; Configuration &gt; Settings page.</p>

## Class of Service Subscriber Settings

Class of service subscriber settings allow you to:

- View the total number of subscribers assigned to a COS.
- View a list of subscribers assigned to a COS.
- Reassign one or more subscribers to another COS.
- Assign one or more subscribers to the COS.

The number of subscribers assigned to a COS can be important if the members are given rights to a licensed feature. To confirm that the number of subscribers does not exceed the number of licenses, see the System > Licensing > License Counts page.

Use the following table to learn more about COS subscriber settings.

Table 14-2 *Subscribers > Class of Service > Subscribers Page*

Field	Considerations
Total Subscribers Assigned to <Name of COS>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• View—Display a list of subscribers who are members of the COS.</li> <li>• Reassign—Reassign one or more subscribers to another COS.</li> <li>• Assign—Add one or more subscribers to the COS.</li> </ul>
Type a <Name of COS> Subscriber to Find	<p>Enter several characters of the name, and click Find. Or enter * to list all subscribers.</p> <p>When Assign is selected, Cisco Unity searches all subscribers in the organization. When View or Reassign is selected, the search is narrowed to subscribers assigned to the specified class of service.</p>
Matching <Name of COS> Subscribers	<p>A list of names that match the characters you entered in Type a &lt;Name of COS&gt; Subscriber to Find.</p> <p>To select several nonsequential names at one time, hold down the Ctrl key while selecting.</p> <p>To select several names in sequence, hold down the Shift key, select the first name in the sequence, and then select the last name in the sequence.</p>

# Class of Service System Access Settings

Class of service system access settings specify which tasks, if any, subscribers—including other system administrators—can do in the Cisco Unity Administrator. You can customize access to Cisco Unity in several ways. For example, you can deny access to the Cisco Unity Administrator, or to specific pages in the Cisco Unity Administrator, such as COS, subscriber, or distribution list pages.

When you deny access to specific pages in the Cisco Unity Administrator, the links for these pages are disabled for the subscriber. Alternatively, you can specify read, edit, add, or delete privileges for these pages, or can allow subscribers access to subscriber pages only for the purpose of unlocking subscriber accounts or changing subscriber passwords.

Note that when the Cisco Unity Administrator uses the Integrated Windows authentication method, a subscriber who has a disabled Active Directory account or who does not have a Windows domain account cannot access the Cisco Unity Administrator or the Status Monitor—even if the subscriber has the proper class of service privileges needed to access them. The same is true when the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method and administrators use their Windows domain account credentials to access them. When you use either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator to create a subscriber, Cisco Unity does not enable an Active Directory account if it is disabled, nor does it create a Windows domain account for a user if one does not already exist.

As necessary, you can use GrantUnityAccess to associate a subscriber account with a Windows domain account, which will allow an administrator to access the Cisco Unity Administrator. You can also use GrantUnityAccess to grant one or more Windows domain accounts access to the Cisco Unity Administrator on one or more Cisco Unity servers without adding a new subscriber account for each one. Alternatively, if administrators will likely use their Domino credentials to log on to the Cisco Unity Administrator, you can use GrantUnityAccess to associate the Domino account of each administrator with a subscriber account that has COS rights to the Cisco Unity Administrator on a particular server. For more details, see the [“About the Accounts That Can Be Used to Administer Cisco Unity” section on page 2-11](#).

Use the following table to learn more about COS system access settings.

**Table 14-3** *Subscribers > Class of Service > System Access Page*

Field	Considerations
Cisco Unity Administrator Application Access	Check this check box to give subscribers assigned to this COS access to the Cisco Unity Administrator. Use the check boxes below this setting to indicate the level of access.
Class of Service	<p>Select the applicable settings for subscribers assigned to this COS:</p> <ul style="list-style-type: none"> <li>• Read—Check this check box to give subscribers read-only access to the Subscribers &gt; Class of Service pages of the Cisco Unity Administrator.</li> <li>• Edit—Check this check box to allow subscribers to edit Subscribers &gt; Class of Service pages of the Cisco Unity Administrator.</li> <li>• Add—Check this check box to allow subscribers to edit Subscribers &gt; Class of Service pages of the Cisco Unity Administrator, and add new ones.</li> <li>• Delete—Check this check box to allow subscribers to edit Subscribers &gt; Class of Service pages of the Cisco Unity Administrator, and delete them.</li> </ul> <p>These fields are unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>

Table 14-3 Subscribers &gt; Class of Service &gt; System Access Page (continued)

Field	Considerations
Directory Handler	<p>Select the applicable settings for subscribers assigned to this COS:</p> <ul style="list-style-type: none"> <li>• Read—Check this check box to give subscribers read-only access to directory handler pages of the Cisco Unity Administrator.</li> <li>• Edit—Check this check box to allow subscribers to edit directory handler pages of the Cisco Unity Administrator.</li> <li>• Add—Check this check box to allow subscribers to edit directory handler pages and create new directory handlers by using the Cisco Unity Administrator.</li> <li>• Delete—Check this check box to allow subscribers to edit directory handler pages and delete directory handlers by using the Cisco Unity Administrator.</li> </ul> <p>These fields are unavailable when the Cisco Unity Administrator Application Access check box is unchecked, or when the Can Unlock Subscriber Accounts and Change Passwords check box is checked.</p>
Subscribers	<p>Select the applicable settings for subscribers assigned to this COS:</p> <ul style="list-style-type: none"> <li>• Read—Check this check box to give subscribers read-only access to subscriber pages of the Cisco Unity Administrator.</li> <li>• Edit—Check this check box to allow subscribers to edit subscriber pages of the Cisco Unity Administrator.</li> <li>• Add—Check this check box to allow subscribers to edit subscriber pages and create new subscribers by using the Cisco Unity Administrator.</li> <li>• Delete—Check this check box to allow subscribers to edit subscriber pages and delete subscribers by using the Cisco Unity Administrator.</li> </ul> <p>These fields are unavailable when the Cisco Unity Administrator Application Access check box is unchecked, or when the Can Unlock Subscriber Accounts and Change Passwords check box is checked.</p>
Can Unlock Subscriber Accounts and Change Passwords	<p>Check this check box to allow subscribers assigned to this COS to edit the necessary fields on subscriber pages in order to unlock subscriber accounts, and to change subscriber passwords. For all other fields on the subscriber pages, read-only access is permitted.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked, or when the Subscribers Access Read, Edit, Add, or Delete check boxes are checked.</p>
Public Distribution Lists	<p>Select the applicable settings for subscribers assigned to this COS:</p> <ul style="list-style-type: none"> <li>• Read—Check this check box to give subscribers read-only access to the public distribution lists pages of the Cisco Unity Administrator.</li> <li>• Edit—Check this check box to allow subscribers to edit the public distribution lists pages of the Cisco Unity Administrator.</li> <li>• Add—Check this check box to allow subscribers to edit the public distribution lists pages of the Cisco Unity Administrator, and to add new public distribution lists.</li> <li>• Delete—Check this check box to allow subscribers to edit the public distribution lists pages of the Cisco Unity Administrator, and to delete public distribution lists.</li> </ul> <p>These fields are unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>

**Table 14-3** *Subscribers > Class of Service > System Access Page (continued)*

<b>Field</b>	<b>Considerations</b>
Schedules and Holidays	<p>Check this check box to give subscribers assigned to this COS access to the System &gt; Schedules page and the System &gt; Holidays page of the Cisco Unity Administrator.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Restriction Tables Access	<p>Check this check box to give subscribers assigned to this COS access to the Subscribers &gt; Class of Service &gt; Restriction Tables page of the Cisco Unity Administrator. Restriction tables limit the phone numbers that subscribers can enter for call transfer, message notification, and fax settings.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Routing Tables Access	<p>Check this check box to give subscribers assigned to this COS access to the Call Management &gt; Call Routing pages of the Cisco Unity Administrator. Call routing tables control the treatment and destinations of incoming calls, based on factors such as trunk, port, and dialed number.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Call Handlers Access	<p>Check this check box to give subscribers assigned to this COS access to the Call Management &gt; Call Handlers pages of the Cisco Unity Administrator.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Status Monitor Access	<p>Check this check box to give subscribers assigned to this COS access to the Status Monitor. The Status Monitor shows real-time information about Cisco Unity.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Reports Access	<p>Check this check box to give subscribers assigned to this COS access to the Reports pages of the Cisco Unity Administrator.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Network Access	<p>Check this check box to give subscribers assigned to this COS access to the Network pages of the Cisco Unity Administrator.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>
Diagnostics Access	<p>Check this check box to give subscribers assigned to this COS access to diagnostic tools on the System &gt; Tools &gt; Diagnostic Traces page.</p> <p>Inform subscribers assigned to the COS that running diagnostic traces can slow system performance. Typically, you run diagnostic traces only when troubleshooting a problem.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>

**Table 14-3** *Subscribers > Class of Service > System Access Page (continued)*

Field	Considerations
Technician Functions Access (Configuration, Licensing, Ports, and Integration Pages)	<p>Check this check box to give subscribers assigned to this COS access to the System Settings pages of the Cisco Unity Administrator.</p> <p>Inform subscribers assigned to the COS to take care when making changes to the Configuration Settings, Ports, and Integration pages because incorrect settings can cause Cisco Unity to malfunction.</p> <p>Unavailable when the Cisco Unity Administrator Application Access check box is unchecked.</p>

## Class of Service Call Transfer Settings

Class of service call transfer settings specify whether subscribers can use the Cisco Unity Assistant to change call screening and call holding options. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

Use the following table to learn more about COS call transfer settings.

**Table 14-4** *Subscribers > Class of Service > Transfer Page*

Field	Considerations
Subscribers Can Change Call Screening Options	<p>Check this check box to give subscribers assigned to this COS the ability to change their own call screening options by using the Cisco Unity Assistant. Call screening options are listed under Gather Caller Information on the Subscribers &gt; Subscribers &gt; Call Transfer page.</p> <p>You may want to allow this option sparingly. Call screening increases the time necessary to transfer unidentified callers to an extension.</p>
Subscribers Can Change Call Holding Options	<p>Check this check box to give subscribers assigned to this COS the ability to change their own call holding options by using the Cisco Unity Assistant. Call holding options are listed under If the Call Is Busy on the Subscribers &gt; Subscribers &gt; Call Transfer page.</p>

## Class of Service Messages Settings

Class of service messages settings specify the maximum length of messages, and whether subscribers can send messages to public distribution lists, and use the live reply feature.

For some integrations, you can set up Cisco Unity so that as a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. By default, the warning tone is disabled. To enable it, see the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19.

When live reply is enabled, subscribers listening to messages by phone can reply to a subscriber message by pressing 4-4 to have Cisco Unity call the subscriber directly. (Subscribers using Optional Conversation 1 press 8-8 for live reply.) Cisco Unity dials the extension of the subscriber who left the message only when:

- The subscriber who left the message is homed on the same Cisco Unity server as the subscriber attempting to reply.

- The Transfer Incoming Calls to Subscriber's Phone setting for the subscriber who left the message is set to ring an extension or another number. (The Transfer Incoming Calls to Subscriber's Phone field is on the Subscribers > Subscribers > Call Transfer page in the Cisco Unity Administrator.) Cisco Unity plays the subscriber greeting or the Opening Greeting when the phone of the subscriber who left the message is busy or the subscriber does not answer.

Consider informing subscribers when you enable this feature, because even when it is enabled, the live reply option is not mentioned in the main Cisco Unity phone menus. It is mentioned in the Help menu for the Cisco Unity phone conversation, the *Cisco Unity User Guide*, and *Cisco Unity at a Glance* card.

Use the following table to learn more about COS messages settings.

**Table 14-5 Subscribers > Class of Service > Messages Page**

Field	Considerations
Maximum Length of Message that Subscribers Can Record in Seconds	Select the length allowed to subscribers assigned to this COS for recording messages and conversations. The default setting is 300 (5 minutes), and the system maximum is 1200 (20 minutes).  The maximum recording length of messages left by unidentified callers is set on the Subscribers > Subscribers > Messages page.  If enabled, a warning tone will sound before the maximum message length is reached.
Subscribers Can Send Messages to Public Distribution Lists	Check this check box to allow subscribers to send messages to public distribution lists.
Subscribers Can Reply to Messages from Other Subscribers by Calling Them	Check this check box to allow subscribers to use the live reply feature. When this check box is checked, subscribers can press 4-4 after listening to a subscriber message, and Cisco Unity will call the subscriber who left the message. (Subscribers who use Optional Conversation 1 can press 8-8 to use live reply.)  When this check box is unchecked, live reply is disabled in the subscriber phone conversation.

## Class of Service Greetings Settings

The class of service greetings setting specifies the maximum length of greetings.

Use the following table to learn more about COS greetings settings.

**Table 14-6 Subscribers > Class of Service > Greetings Page**

Field	Considerations
Maximum Greeting Length in Seconds	Select the recording length allowed to subscribers assigned to this COS for recording greetings.  The range is 1 to 999 seconds; the default is 90 seconds.  If enabled, a warning tone will sound before the maximum greeting length is reached.

## Class of Service Features Settings

Class of service features settings specify which Cisco Unity features the subscribers in this COS can use.

Note that when a COS includes access to an application that requires individual licenses, you can add subscribers to the COS only if enough licenses are available.

Use the following table to learn more about COS features settings.

**Table 14-7** *Subscribers > Class of Service > Features Page*

Field	Considerations
FaxMail	<p>Check this check box to allow subscribers assigned to this COS to manage their fax messages over the phone, which includes having their fax and e-mail messages delivered to a fax machine. The permission granted by checking this check box applies only to managing faxes over the phone. All subscribers, regardless of COS, can manage fax messages in their Inboxes.</p> <p>To allow subscribers assigned to this COS to have their e-mail messages delivered to a fax machine, you must select the check boxes for both Text to Speech e-mail and for FaxMail.</p>
Text to Speech for E-Mail Messages	<p>Check this check box to allow subscribers assigned to this COS to have their e-mail messages read to them by an e-mail reader over the phone.</p> <p>To allow subscribers to have their e-mail messages delivered to a fax machine, you must select both the check boxes for Text to Speech e-mail and for FaxMail.</p>
Cisco Unity Assistant	<p>Check this check box to allow subscribers assigned to this COS to use the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)</p>

## Class of Service Restriction Table Settings

Class of service restriction table settings specify which restriction tables are used for message delivery, call transfer, and fax delivery for subscribers in this COS.

See the [“Overview: Restriction Tables”](#) section on page 25-1 for more information about restriction tables.

Use the following table to learn more about COS restriction table settings.

**Table 14-8** *Subscribers > Class of Service > Restriction Tables Page*

Field	Considerations
Select a Restriction Table	<p>Select a restriction table for each of the following:</p> <ul style="list-style-type: none"> <li>• <b>Outcalling</b>—Select a restriction table to limit phone numbers that subscribers assigned to this COS can enter in message delivery settings. The table you select also restricts the subscriber extensions that Cisco Unity dials when the phone is selected as the recording and playback device for the Media Master.</li> <li>• <b>Transfers</b>—Select a restriction table to limit phone numbers that subscribers assigned to this COS can enter in call transfer settings.</li> <li>• <b>Fax</b>—Select a restriction table to limit phone numbers that subscribers assigned to this COS can enter in fax dialing settings.</li> </ul> <p>Note that when you click the View link for any of these tables, you leave the Subscribers &gt; Class of Service &gt; Restriction Tables page, and move to the Call Management &gt; Restriction Tables page.</p>







## Creating Subscriber Accounts

---

### Overview: Creating Subscriber Accounts

Anyone who has an account on Cisco Unity is a subscriber. You create regular and Internet subscriber accounts by using either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator.

If you are planning to create subscriber accounts for administrators to use when accessing the Cisco Unity Administrator, first review the [“About the Accounts That Can Be Used to Administer Cisco Unity”](#) section on page 2-11, and then return to this chapter.

#### Creating Regular Subscriber Accounts

To learn more about creating regular subscriber accounts, see the following sections in this chapter:

- [Before Creating Regular Subscriber Accounts, page 15-2](#)—This section describes the issues that you must consider before creating subscriber accounts.
- [About Regular Subscriber Accounts and Data Storage, page 15-4](#)—This section describes how creating subscriber accounts works, and where Cisco Unity stores subscriber account information.
- [Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts, page 15-5](#)—This section provides information about using the Cisco Unity Bulk Import wizard to create regular subscriber accounts by importing user data from the Domino directory or from a CSV file.
- [Using the Cisco Unity Administrator to Create Individual Subscriber Accounts, page 15-16](#)—This section provides information about using the Cisco Unity Administrator to create a regular subscriber account by importing existing user data from Domino.
- [After Creating Subscriber Accounts, page 15-18](#)—This section lists the tasks to consider once you have created Cisco Unity subscriber accounts.

#### Creating External Subscriber Accounts

To create Internet subscribers, refer to the “Task List: Setting Up Internet Subscribers” in the “Internet Subscribers” chapter in the *Networking in Cisco Unity Guide*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/net/net403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net403/dom/index.htm)).

# Before Creating Regular Subscriber Accounts

This section lists—in order—the issues that you must consider before creating subscriber accounts. If you are creating subscriber accounts that you want to use to administer Cisco Unity, you should review the “[About the Accounts That Can Be Used to Administer Cisco Unity](#)” section on page 2-11 in addition to the information that follows.

## 1. Cisco Unity Configuration and Permissions

If you are unsure whether the account that you are using has sufficient rights and permissions to create subscriber accounts, or whether Cisco Unity is properly configured to work with your message store, use the following procedure to run the SysCheck diagnostic tool.

### To Check Cisco Unity Setup and Permissions by Using the Cisco Unity SysCheck Tool

- 
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **SysCheck**.
- Step 3** On the Welcome to the Cisco Unity Configuration Wizard page, click **Select Configuration Tests**, and click **Next**.
- Step 4** Uncheck the boxes for the message stores that are not connected to Cisco Unity.
- Step 5** Click **Test**.
- Step 6** In the Test Results box, click the link provided to view the test results.
- Step 7** If no errors are reported, proceed to [Step 8](#). Otherwise, do the following sub-steps:
- a. Follow the advice offered in the Resolution column to correct each configuration or permissions error.
  - b. Return to the Completing the Check Unity Configuration Wizard page, and click **Finish**.
  - c. Repeat [Step 2](#) through [Step 7](#) until no errors are reported.
- Step 8** Click **Finish**.
- 

## 2. Licenses

Confirm that you have the Cisco Unity user licenses that are required for the type of subscriber accounts that you plan to create. You can view the number of licenses purchased, and the number that are used and unused on your system, from the System > Licensing page in the Cisco Unity Administrator. If you need additional licenses, contact your reseller. If you need to upgrade your licenses, refer to the “Adding Cisco Unity User Licenses” section in the “Modifying the Cisco Unity 4.0 System” chapter of the *Cisco Unity Installation Guide*. (The *Cisco Unity Installation Guide* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/inst/inst403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst403/dom/index.htm).)

## 3. Account Policies

Account policies govern subscriber passwords and account lockouts for all Cisco Unity subscriber accounts. There are two account policies that you can set up to secure how subscribers access Cisco Unity:

- See the “[Account Policy Settings](#)” chapter to set up system-wide phone password and lockout policies that apply when subscribers access Cisco Unity by phone.

- See the [“About Cisco Unity Administrator Authentication”](#) section on page 2-5 to set up system-wide logon, password, and lockout policies that apply when subscribers use Cisco Unity web applications such as the Cisco Personal Communications Assistant (PCA) to access Cisco Unity.

Each account policy has default settings, which you can modify in the Cisco Unity Administrator.

(Subscribers use the Cisco PCA to access the Cisco Unity Assistant. Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

#### 4. Enhanced Phone Security

You can set up Cisco Unity subscriber accounts to use a secure logon method when subscribers access Cisco Unity by phone. See the [“Enhanced Phone Security”](#) chapter for information on setting up enhanced phone security, if desired. If you choose to set up enhanced phone security, then you must also create a new class of service or modify an existing one for the subscribers who will be using enhanced phone security (see the next task).

#### 5. Classes of Service

A class of service (COS) defines limits and permissions for subscribers who use Cisco Unity. For example, a COS:

- Controls access to the Cisco Unity Administrator and to features such as Text to Speech e-mail.
- Controls how subscribers interact with Cisco Unity. For example, a COS dictates the maximum length of subscriber messages and greetings, whether subscribers can choose to be listed in directory assistance, whether subscribers use a secure logon method to access Cisco Unity by phone, and whether subscribers can send messages to a public distribution list.
- Specifies the restriction table used to control the phone numbers subscribers can use for fax delivery, message notification, call transfer, and other tasks.

In the Cisco Unity Administrator, a COS is specified in each subscriber template; thus, a subscriber is assigned to the COS which is specified in the template upon which the subscriber account is based. Cisco Unity includes predefined classes of service, which you can modify. You can also create new classes of service. For details, see the [“Class of Service Settings”](#) chapter.

#### 6. Restriction Tables

Restriction tables in the Cisco Unity Administrator allow you to control the phone numbers that subscribers and administrators can use for:

- Transferring calls
- Recording and playback by phone from Cisco Unity applications, when the phone is the designated recording and playback device in the Media Master or in the VCR-style player/recorder available in Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity (the Media Master is available in the Cisco Unity Administrator and the Cisco Unity Assistant)
- Delivering faxes to a fax machine
- Sending message notifications

Each class of service specifies a restriction table for call transfers, one for message notification, and one for fax deliveries. Cisco Unity comes with predefined restriction tables, which you can modify. See the [“Restriction Tables”](#) chapter for details.

#### 7. Public Distribution Lists

Public distribution lists are used to send voice messages to multiple subscribers at the same time. Cisco Unity assigns new subscribers to the public distribution lists that are specified in the template on which the subscriber account is based. The class of service associated with a subscriber account dictates whether that subscriber can use Cisco Unity to send messages to public distribution lists. See the “[Public Distribution List Settings](#)” chapter for details.

### 8. Subscriber Templates

In the Cisco Unity Administrator, you can specify settings for a group of subscribers by using a subscriber template. The settings from the template you choose are applied to subscriber accounts as the accounts are created. Cisco Unity comes with a default subscriber template, which you can modify, and you can create an unlimited number of additional templates.

Subscriber templates contain settings that are applicable for subscribers of a particular type, such as a department. Subscriber template settings also include initial phone passwords for subscribers. To protect Cisco Unity from unauthorized access, you can either change the default phone password before subscriber accounts are created, or you can wait until after you create subscriber accounts to use the Cisco Unity Bulk Import wizard to assign a unique password to each subscriber account that you created. In either case, consider specifying a long—eight or more digits—and non-trivial password. See the “[Subscriber Template Settings](#)” chapter for details.

### 9. Domino Address Books

If you use the Cisco Unity Administrator to create a subscriber account, confirm that the address book(s) listed on the System > Configuration > Subscriber Address Books page in the Cisco Unity Administrator contain the user data that you want to import when you create the subscriber account. If necessary, you can add another address book to the System > Configuration > Subscriber Address Books page. See the “[Subscriber Address Book Settings](#)” section on page 28-7 for details.

## About Regular Subscriber Accounts and Data Storage

This section describes how Cisco Unity subscriber accounts work, and where Cisco Unity stores subscriber account information.

For details, see the following sections:

- [About Subscriber Accounts, page 15-4](#)
- [About Data Storage, page 15-5](#)

## About Subscriber Accounts

Each regular Cisco Unity subscriber account is associated with a Domino Person document. Note that when the Cisco Unity Administrator and the Status Monitor use Integrated Windows authentication, a subscriber who has a disabled Active Directory account or who does not have a Windows domain account cannot access either application—even if the subscriber has the proper class of service privileges needed to access them. The same is true when the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method and administrators will use their Windows domain account credentials to access them.

When you use either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator to create a subscriber account, it is important to note that Cisco Unity does not:

- Import Windows domain account information.
- Enable an Active Directory account if it is disabled.

- Create a Windows domain account for a person if one does not already exist.

Therefore, after you create a subscriber account that will be used to administer Cisco Unity, you must use `GrantUnityAccess` to associate the subscriber account with a Windows domain account that will allow the subscriber to access the Cisco Unity Administrator. For details, see the [“About the Accounts That Can Be Used to Administer Cisco Unity”](#) section on page 2-11.

When the Cisco Unity Administrator and the Status Monitor use Anonymous authentication and administrators will use their Domino credentials to access them, you do not need to create Windows domain accounts for each subscriber account that you create, or use `GrantUnityAccess` to associate the subscriber accounts with a Windows domain account.

## About Data Storage

Subscribers have a Domino mail file in which Cisco Unity stores voice messages. Cisco Unity stores information about subscriber accounts in a SQL database on the Cisco Unity server. In addition, a small subset of the subscriber account information is also stored in the Domino address book.

# Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts

The Cisco Unity Bulk Import wizard allows you to create multiple subscriber accounts at once by either importing user data directly from the Domino directory, or by importing user data contained in a comma-separated value (CSV) file.

See the following sections for detailed information on using the Cisco Unity Bulk Import wizard to create subscriber accounts:

- [Importing User Data Directly from a Message Store Directory, page 15-5](#)
- [Importing User Data from a CSV File, page 15-6](#)
- [Running the Cisco Unity Bulk Import Wizard, page 15-14](#)
- [Correcting Import Errors, page 15-15](#)

## Importing User Data Directly from a Message Store Directory

When you use the Cisco Unity Bulk Import wizard to import user data directly from the message store directory, Cisco Unity utilizes the mailbox data and Windows domain account information to create the Cisco Unity subscriber account. However, the Cisco Unity Bulk Import wizard does not:

- Import Windows domain account information.
- Enable an Active Directory account if it is disabled.
- Create a Windows domain account for a person if one does not already exist.

This is important to note if subscribers will use Windows credentials to access the Cisco Unity Administrator and the Status Monitor. For more details, see the [“About Subscriber Accounts”](#) section on page 15-4.

Finally, the Cisco Unity Bulk Import wizard requires each regular subscriber to have a `DTMF_ACCESS_ID` that callers can use to reach the subscriber. Typically, the `DTMF_ACCESS_ID` is the same as the subscriber extension. Before running the Cisco Unity Bulk Import wizard, print out a list

of the user names that you plan to import, and specify a DTMF\_ACCESS\_ID for each user. The ID must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one. Save this list to use when you enter any missing DTMF\_ACCESS\_IDs during the import process.

When you are ready to create subscribers by importing user data directly from the message store directory, see the [“Running the Cisco Unity Bulk Import Wizard” section on page 15-14](#).

## Importing User Data from a CSV File

CSV is a common text file format for moving data from one data store to another. In particular, importing from a CSV file is helpful when you want to create subscriber accounts based on user data from voice messaging systems that run on different operating systems, or that have different database structures than Cisco Unity. As long as the user data presented in a CSV file is formatted as indicated in this section, you can use it to create subscribers with existing Domino Person documents.

Note that when the Cisco Unity Bulk Import wizard creates a subscriber account, it does not:

- Import Windows domain account information for a person.
- Enable an Active Directory account if it is disabled.
- Create a Windows domain account for a person if one does not already exist.

This is important to note if subscribers will use Windows credentials to access the Cisco Unity Administrator and the Status Monitor. For more details, see the [“About Subscriber Accounts” section on page 15-4](#).

The first row in your CSV file must contain column headers that identify the type of data in each column; information in the subsequent rows must contain the data that you want to import. Column headers must be in uppercase, separated by commas, and spelled as shown in the tables in the following sections:

- [Required Column Headers, page 15-6](#)
- [Optional Column Headers, page 15-7](#)



### Note

In addition, make sure that commas separate the data in each row in your CSV file, including the column headers in the first row. Do not use a tab, spaces, or a semicolon to separate values in the file. Finally, if any data includes a space, quotes, or commas, contain it within quotes.

### Required Column Headers

The required column headers for regular subscribers are shown in [Table 15-1](#). Note that the column headers are shown in the order in which they should appear in your CSV file.

**Table 15-1 Required CSV Headers for Regular Subscribers**

Column Header	Description
LAST_NAME	Subscriber last name. Enter any combination of letters, digits, spaces, apostrophes, and dashes, up to a maximum of 32 characters.
FIRST_NAME	Subscriber first name. Enter any combination of letters, digits, spaces, apostrophes, and dashes, up to a maximum of 32 characters.

**Table 15-1 Required CSV Headers for Regular Subscribers (continued)**

Column Header	Description
DTMF_ACCESS_ID	<p>The number that callers dial to reach a subscriber. This value corresponds to the Extension field on the Subscribers &gt; Subscribers &gt; Profile Page page in the Cisco Unity Administrator.</p> <p>Enter any combination of digits from 0 to 9, up to a maximum of 40 digits. Do not include any spaces. Note that the value must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.</p>
SHORT_NAME	<p>The unique name that is created by the Domino Administrator to represent each Domino Person document within a domain. The short name is usually represented by the first initial and last name of the user.</p> <p>Enter any combination of letters or digits, up to a maximum of 64 characters. Do not include any spaces. The data that you enter here must be valid short name in the Domino Administrator.</p>

### Optional Column Headers

There are a number of optional column headers that you can include in your CSV file, as shown in [Table 15-2](#). Most optional column headers correspond to subscriber settings defined in the subscriber template, including class of service (COS), call transfer, and message notification settings. When data for a particular subscriber setting is not included in the CSV file, the Cisco Unity Bulk Import wizard uses settings in the subscriber template that you choose when you run the Cisco Unity Bulk Import wizard. For this reason, you should review the settings in the subscriber template that you will use to create the accounts before adding any of the optional column headers to your CSV file. See the [“Subscriber Template Settings”](#) chapter for more information about subscriber templates.

Use the following table to learn more about the optional column headers that you can include in the CSV file. Unless otherwise indicated, all optional column headers can be used to define any type of subscriber account.

**Table 15-2 Optional CSV File Column Headers**

Optional Column Header	Description
ALTERNATE_EXTENSION_1	<p>In addition to the “primary” extension that you assign subscribers, you can also assign subscribers alternate extensions.</p> <p>For example, if you have more than one Cisco Unity server that accesses a single, corporate-wide directory, you may want to add alternate extensions so that a subscriber uses the same number when addressing a message to a subscriber associated with another Cisco Unity server and when calling that subscriber directly. (For more information on using alternate extensions as addressing options with Digital Networking, refer to the <i>Networking in Cisco Unity Guide</i>.)</p> <p>Even if assigning alternate extensions is not necessary in your situation, you may want to add them as a convenience for subscribers. For example, alternate extensions can be used to:</p> <ul style="list-style-type: none"> <li>• Handle multiple line appearances on subscriber phones.</li> <li>• Offer easy message access on direct calls from a certain phones.</li> <li>• Simplify addressing messages to subscribers at different locations.</li> <li>• Enable alphanumeric extensions in Cisco Unity for an integration with a SIP phone system.</li> </ul> <p>Each alternate extensions must be unique—up to the dialing domain level, if applicable—and no more than 40 characters in length.</p> <p>Enter any combination of digits 0 through 9, or if you have a SIP integration, enter letters a through z. Do not use spaces, dashes, or parentheses between characters.</p>
AUDIO_SPEED	<p>Defines the speed of message playback.</p> <ul style="list-style-type: none"> <li>• 0—low speed.</li> <li>• 100—medium speed (default value).</li> <li>• 200—fast speed.</li> </ul>
AUDIO_VOLUME	<p>Indicates the volume for message playback.</p> <ul style="list-style-type: none"> <li>• 0—low volume.</li> <li>• 50—medium volume (default value).</li> <li>• 100—high volume.</li> </ul>
CALLERS_LANGUAGE	<p>The language of the Cisco Unity conversation that the caller hears when they call a subscriber.</p> <p>Enter any combination of letters and digits, up to a maximum of four characters.</p>
CONVERSATION_NAME	<p>The Cisco Unity conversation that the subscriber hears when retrieving messages.</p> <p>Enter any combination of letters and digits, up to a maximum of 64 characters.</p>

Table 15-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
COS_OBJECT_NAME	<p>The name of the subscriber class of service (COS) of which the subscriber will be a member. The COS must already exist in the Cisco Unity Administrator.</p> <p>Enter any combination of letters, digits, and braces, up to a maximum of 128 characters. Enter the name of the COS as it appears in the Cisco Unity Administrator.</p>
DISPLAY_NAME	<p>If the display name is not specified, it is constructed from the first and last names based on the rule in the subscriber template selected during the import.</p> <p>Enter any combination of letters, digits, spaces, periods, commas, apostrophes, or other characters—including dashes, up to a maximum of 64 characters.</p>
DTMF_ACCESS_ID <i>(optional for Internet subscribers only; required for regular subscribers)</i>	<p>The number that callers dial to reach a subscriber. This is also the extension that subscribers on the local Cisco Unity server use to address messages to Internet subscribers.</p> <p>This value corresponds to the Extension field on the Subscribers &gt; Subscribers &gt; Profile Page page in the Cisco Unity Administrator.</p> <p>Enter any combination of digits from 0 to 9, up to a maximum of 40 digits. Do not include any spaces. Note that the value must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.</p>
DTMF_PASSWORD	<p>The password that governs how subscribers initially log on to Cisco Unity by phone.</p> <p>This value corresponds to the Password field on the Subscribers &gt; Subscriber &gt; Passwords page in the Cisco Unity Administrator. By default, subscriber templates use 12345 as the initial phone password for all subscribers unless you change it in the template or change it here.</p> <p>Enter any combination of digits 0 through 9, up to a maximum of 20 digits. The minimum length of the password depends on settings on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page in the Cisco Unity Administrator.</p>
LIST_IN_DIRECTORY	<p>Determines whether the subscriber is listed in the phone directory.</p> <ul style="list-style-type: none"> <li>• 0—turns directory listing off.</li> <li>• 1—turns directory listing on.</li> </ul>
MAX_MSG_LENGTH	<p>Indicates the maximum length of voice mail messages (in seconds) that unidentified callers can leave.</p> <p>Enter any value from 0 to 999 seconds.</p>
MWI_EXTENSION_1	<p>The message waiting indicator (MWI) extension, if different from phone extension for the subscriber.</p> <p>Enter any combination of digits from 0 to 9 for the extension (or if you have a SIP integration, enter letters a through z), and “,” (comma) or “;” (semi-colon) for pause, for a maximum of 40 characters.</p>
NOTES	<p>The Cisco Unity Bulk Import wizard ignores a column with this header. The Cisco Unity Bulk Import wizard does not support more than one NOTES column in a CSV file.</p> <p>Enter any comments that you may have for this record. Enter any combination of letters, characters, and digits, for a maximum of 255 characters.</p>

Table 15-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
PAGER1_NUMERIC_AFTER_DIAL_DIGITS <i>(regular subscribers only)</i>	<p>The extra digits that Cisco Unity dials after the phone number for a message notification. The extra digits are shown on the pager display.</p> <p>This column corresponds to the Extra Digits field for the Pager device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator.</p> <p>Enter any combination of digits from 0 to 9, up to a maximum of 32 digits.</p>
PAGER1_NUMERIC_DIAL_DELAY <i>(regular subscribers only)</i>	<p>Specifies the number of seconds to wait before dialing the extra digits specified in the PAGER1_NUMERIC_AFTER_DIALDIGITS column. Use this option if the automatic call progress detection of your phone system is not reliable (for example, if you experience noisy phone lines and unusual ringing patterns).</p> <p>This column corresponds to the Seconds to Wait Before Dialing Extra Digits field for the Pager device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator.</p> <p>Enter any value from 0 to 100 seconds.</p>
PAGER1_NUMERIC_DISABLE	<p>Disables the numeric pager device. This column corresponds to the Status field for the Pager device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator.</p> <p>Enter 1.</p> <p>After you create the subscriber accounts, you can enable the pager in the Cisco Unity Administrator, or you can tell subscribers to do so in the Cisco Unity Assistant.</p>
PAGER1_NUMERIC_PHONE_NO <i>(regular subscribers only)</i>	<p>The phone number, including trunk access code, of the numeric pager to be used for message notifications.</p> <p>This column corresponds to the Phone Number field for the Pager device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled upon import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant.</p> <p>Enter any combination of digits 0 through 9 and the following dialing characters, up to a maximum of 40 characters:</p> <ul style="list-style-type: none"> <li>• , (comma) to insert a one-second pause.</li> <li>• # and * to correspond to the # and * keys on the phone.</li> </ul>
PAGER1_TEXT_AFTER_DIAL_DIGITS <i>(regular subscribers only)</i>	<p>Specifies a phone number if the subscriber has a text-compatible cell phone and wants text pager notifications to include a “From” or “Return Call” phone number. Typically, this field contains the number of the Cisco Unity server that the subscriber calls to check messages.</p> <p>The From phone number appears in the last line of any text pager notification. A subscriber can press the Return Call button on many text-compatible cell phones to dial the phone number. The cell phone must support automatic callback in order to use this feature.</p> <p>This column corresponds to the From: (Phone Number) field for the Text Pager 1 device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator.</p> <p>Enter any combination of digits, up to a maximum of 32 digits.</p>

Table 15-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
PAGER1_TEXT_DISABLE	<p>Disables the text pager device. This column corresponds to the Status field for the Text Pager 1 device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator.</p> <p>Enter 1.</p> <p>After you create the subscriber accounts, you can enable the pager in the Cisco Unity Administrator, or you can tell subscribers to do so in the Cisco Unity Assistant.</p>
PAGER1_TEXT_SMTP_ADDRESS <i>(regular subscribers only)</i>	<p>Specifies the e-mail address of the text pager, text-compatible cell phone, or another e-mail account (such as a home e-mail address) to which message notifications will be sent.</p> <p>This column corresponds to the To: (E-Mail Address) field for the Text Pager 1 device on the Subscribers &gt; Subscribers &gt; Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled upon import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant.</p> <p>Enter any combination of letters, digits, colons, ampersands, dashes, periods, and underscores, up to a maximum of 128 characters.</p>
PUBLIC_DL	<p>Specifies the public distribution lists to which new subscribers are added.</p> <p>This column corresponds to the Subscribers &gt; Subscriber &gt; Distribution Lists page in the Cisco Unity Administrator. By default, subscriber templates assign new subscribers to the All Subscribers list. Use this column to add subscribers to distribution lists that are not already specified in the template; any lists that you enter in this column do not overwrite the lists specified in the template.</p> <p>Enter any combination of letters, digits, space, period, semicolon, comma, or most other characters—including apostrophe and underscores, up to 255 characters. Separate each public distribution list name by a semicolon.</p> <p>For example, you can enter “All Subscribers; Accounting Department.”</p>
SUBSCRIBER_TEMPLATE	<p>The subscriber template that you want to associate the subscribers with once they are created. Enter any combination of letters and digits, up to a maximum of 128 characters.</p>
SUBSCRIBERS_LANGUAGE	<p>The language that the subscriber hears when logging on to Cisco Unity by phone. Enter any combination of letters and digits, up to a maximum of four characters.</p>
TIME_EXPIRES	<p>Specifies the date that call transfer is turned off for the subscriber extension. If the value is 0 (zero), call transfer is turned on, and because there is no expiration date, it never turns off. If the value is a date in the past (for example, 01/01/80), call transfer is turned off.</p> <p>Enter a valid date in the format of mm/dd/yy, yy/mm/dd, or enter 0 (zero).</p>

Table 15-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
TRANSFER_STRING	<p>Specifies the call transfer number for the subscriber. The value is usually the same as the DTMF_ACCESS_ID (so Cisco Unity sends calls to the subscriber extension), though the value for the dialing transfer string can be left blank.</p> <p>This corresponds to the Transfer Incoming Calls to Subscriber's Phone field on the Subscribers &gt; Subscribers &gt; Call Transfer Page in the Cisco Unity Administrator.</p> <p>Enter any combination of digits from 0 to 9 up to a maximum of 40 digits, and the following dialing characters:</p> <ul style="list-style-type: none"> <li>• , (comma) to insert a one-second pause.</li> <li>• ; (semi-colon) to insert a pause.</li> </ul>
USE_BRIEF_PROMPTS	<p>Indicates whether the subscriber hears brief or full phone menus when accessing Cisco Unity over the phone.</p> <ul style="list-style-type: none"> <li>• 0—turns brief menus on.</li> <li>• 1—turns full menus on.</li> </ul>
XFER_ANNOUNCE	<p>Defines whether Cisco Unity says “transferring call” when the phone is answered on an incoming external call. For this to work, XFER_TYPE must be set to “supervised.”</p> <ul style="list-style-type: none"> <li>• 0—turns announce off.</li> <li>• 1—turns announce on.</li> </ul>
XFER_CONFIRM	<p>Defines whether Cisco Unity asks subscribers if they would like to take calls. For this to work, XFER_TYPE must be set to “supervised.”</p> <ul style="list-style-type: none"> <li>• 0—turns confirm off.</li> <li>• 1—turns confirm on.</li> </ul>
XFER_HOLDING_MODE	<p>Determines if the caller can be put on hold when an extension is busy. For this to work, XFER_TYPE must be set to “supervised.”</p> <ul style="list-style-type: none"> <li>• 0—turns call holding off.</li> <li>• 1—turns call holding on.</li> </ul>
XFER_INTRODUCE	<p>Defines whether subscribers hear “call for &lt;the recorded voice name of the subscriber&gt;,” or “call for &lt;extension number&gt;” when they answer an incoming external call. Used when two or more subscribers share a phone. For this to work, XFER_TYPE must be set to “supervised.”</p> <ul style="list-style-type: none"> <li>• 0—turns introduce off.</li> <li>• 1—turns introduce on.</li> </ul>
XFER_RINGS	<p>When doing a supervised transfer, the number of rings to wait before activating the appropriate call handler.</p> <p>Enter any digit from 1 to 9.</p>
XFER_SCREENING	<p>Sets call screening to off, on, or on with “memory” (the recorded name of the caller is added to the message). For this to work, XFER_TYPE must be set to “supervised.”</p> <ul style="list-style-type: none"> <li>• 0—turns call screening off.</li> <li>• 1—turns call screening on.</li> <li>• 2—turns call screening on with memory.</li> </ul>

**Table 15-2** Optional CSV File Column Headers (continued)

Optional Column Header	Description
XFER_TYPE	Used in conjunction with RNA_ACTION to determine whether Cisco Unity monitors the progress of a call until the subscriber answers the phone. <ul style="list-style-type: none"> <li>0—unsupervised transfer; Cisco Unity does not monitor call progress.</li> <li>1—supervised transfer; Cisco Unity monitors call progress.</li> </ul>
ZERO_KEY_RULE (regular subscribers only)	Specifies the display name for the call handler to which calls to this subscriber are transferred when unidentified callers press “0” during the subscriber greeting. This allows calls to different groups of subscribers to be handled by different operators.  Note that the Import wizard checks to see if the name is a valid call handler, so the call handler must have been created in the Cisco Unity Administrator before doing the import.  Enter any combination of letters, digits, periods, spaces, dashes, or other characters—including underscores, up to a maximum of 128 characters.

After reviewing [Table 15-1](#) and [Table 15-2](#), use the following procedure to prepare your CSV file.

#### To Prepare a CSV File for Creating Regular Subscriber Accounts

- Step 1** Save the data which you will use to create Cisco Unity accounts 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 Cisco Unity Bulk Import wizard imports the data.
- Step 2** Copy the CSV file to the Cisco Unity server or to a folder that you can browse to from the server.
- 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, quotes, or commas, contain it within quotes.
- 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 last name of the user is followed by the first name and then by DTMF\_ACCESS\_ID and the short name:
- ```
Abade,Alex,2001,aabade
Bader,Kelly,2002,kbader
Campbell,Terry,2003,tcampbell
Cho,Li,2004,lcho
```
- Step 5** Enter the required column headers above the first row of data. Column headers must be uppercase, separated by commas, and spelled as indicated in [Table 15-1](#) on page 15-6.
- For example, the column headers for the sample data from [Step 4](#) would look like this:
- ```
LAST_NAME,FIRST_NAME,DTMF_ACCESS_ID,SHORT_NAME
```
- Step 6** If desired, add any of the optional column headers listed in [Table 15-2](#) on page 15-8 to the first row, and the corresponding data that you want to import in the subsequent rows below. As you do so, confirm that:
- Column headers and data are separated by commas. Note that each row does not have to contain data for each optional column header.

- Any data that includes a space, quotes, or commas is contained within quotes.
- 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 Cisco Unity Bulk Import wizard ignores data beneath a NOTES column header, but the wizard does not support more than one NOTES column in a CSV file.
- Step 8** Confirm that each row contains the applicable data corresponding to each column header. See [Table 15-1](#) and [Table 15-2](#) for descriptions of valid data for each column header.
- Step 9** Save the file as a CSV file.
- Step 10** Continue with the procedure in the “[Running the Cisco Unity Bulk Import Wizard](#)” section on [page 15-14](#).
- 

## Running the Cisco Unity Bulk Import Wizard

Do the procedure in this section to use the Cisco Unity Bulk Import wizard to create multiple subscriber accounts. Do so only after you have reviewed the following sections:

- [Before Creating Regular Subscriber Accounts, page 15-2](#)
- [Importing User Data Directly from a Message Store Directory, page 15-5](#) (as applicable)
- [Importing User Data from a CSV File, page 15-6](#) (as applicable)

For best results, note the following:

- Do not attempt to create more than 7,500 new subscriber accounts at once. If you have more than 7,500 users for whom you want to create Cisco Unity subscriber accounts, run the Cisco Unity Bulk Import wizard multiple times.
- Once the wizard has created a subscriber account for a particular user, it will not process the data for that user when it is run again.
- You can only create one type of subscriber each time you run the Cisco Unity Bulk Import wizard.
- The Cisco Unity Bulk Import wizard can only import user data from one message store directory at a time.

When the Cisco Unity Bulk Import wizard initially loads the Domino directory data or the records in your CSV file, it examines the data for errors. If an error is found, the wizard notifies you and logs the error in the error.log file. You can choose either to ignore the error and correct it later, or you can correct the error, and start the wizard again. After it creates subscriber accounts, the wizard displays a dialog box that reports the results of loading the data, including the number of records found, the number of records successfully loaded, and the number of records that still have errors.

Use the following procedure to use the Cisco Unity Bulk Import wizard to create regular subscriber accounts, and to manage any errors that the wizard discovers in the process.



### Note

Before you run the Cisco Unity Bulk Import wizard, disable virus-scanning services and intrusion-detection software on the Cisco Unity server, if applicable. Otherwise, the Cisco Unity Bulk Import wizard may run slowly. See the Cisco Unity Bulk Import wizard online Help for procedures.

### To Create Regular Subscribers by Using the Cisco Unity Bulk Import Wizard

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.
- Step 2** Follow the on-screen instructions presented on each page of the wizard.  
To learn more about the options presented in the dialog boxes that appear as the wizard proceeds, click **Help**.
- Step 3** When prompted to choose the type of subscriber that you want to create, click **Unified Messaging**.
- Step 4** Click **Next**, and proceed through the wizard. If the wizard reports any errors, you can:
- Click **OK** to continue with the import, and fix the errors later.
  - Fix the errors. See the [“Correcting Import Errors” section on page 15-15](#) for details.
- Step 5** If you are importing user data directly from the message store directory, confirm that there is a `DTMF_ACCESS_ID` specified for each user on the Select Data to Import page.  
Enter the applicable data in the grid if a `DTMF_ACCESS_ID` is not specified for a user:
- Enter digits only.
  - Typically, the `DTMF_ACCESS_ID` is the same as the subscriber extension. Therefore, the data you enter should be consistent with the extension numbering plan used in your organization.
  - The ID must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.
- Step 6** Once the subscriber accounts are created, click **Finish**.
- Step 7** If you had import errors, but in [Step 4](#) you chose to correct them later, see the [“Correcting Import Errors” section on page 15-15](#).  
If you had no import errors, or if all errors have now been corrected, see the [“After Creating Subscriber Accounts” section on page 15-18](#).
- 

## Correcting Import Errors

The error log file contains data that the Cisco Unity Bulk Import wizard could not import. The Cisco Unity Bulk Import wizard reports the first error it detects in any user mailbox or row in a CSV file. Once you correct that error, the Cisco Unity Bulk Import wizard may detect additional errors in the same mailbox or row when the data is imported again. Thus, you may need to repeat the correction process—running the Cisco Unity Bulk Import wizard and correcting an error—several times to find and correct all errors.

The output log file contains all the records that were not imported. You can save it as a CSV file, and use it when you run the Cisco Unity Bulk Import wizard again. Note that each time that you run the Cisco Unity Bulk Import wizard, the error and output log files are overwritten (unless you specify a new name for the files each time you run it).

To correct import errors, use one of the two procedures below.

---

**To Correct Errors That Occurred When Importing Data from the Message Store**

---

- Step 1** Go to the directory location of the error log file you specified during the import. (The default location and file name is C:\Error.log.)
  - Step 2** Use a text editor to open the error log file. You will use the error codes in the file to make corrections.
  - Step 3** Double-click a mailbox that contains an error to see the properties.
  - Step 4** Enter corrections in the applicable boxes in the mailbox.
  - Step 5** Click **OK**.
  - Step 6** Repeat [Step 3](#) through [Step 5](#) for each mailbox listed in the error log file.
  - Step 7** Run the Cisco Unity Bulk Import wizard again.
  - Step 8** Repeat this procedure until all subscriber accounts are created without error, and then proceed to the [“After Creating Subscriber Accounts”](#) section on page 15-18.
- 

---

**To Correct Errors That Occurred When Importing Data from a CSV File**

---

- Step 1** Go to the directory location of the error log file you specified during the import. (The default location and file name is C:\Error.log.)
  - Step 2** Use a text editor to open the error log file. You will use the error codes in the file to make corrections.
  - Step 3** Go to the directory location of the output log file you specified during the import. (The default location and file name is C:\Output.log.) This file contains all the records that were not imported.
  - Step 4** Use a text editor to open the output log file.
  - Step 5** Correct any records in the output file that are listed as errors in the error log file.
  - Step 6** When you have finished editing the output log file, save it as a CSV file with a new name.
  - Step 7** Run the Cisco Unity Bulk Import wizard again with the CSV file that you saved in [Step 6](#).
  - Step 8** Repeat this procedure until all subscriber accounts are created without error, and then proceed to the [“After Creating Subscriber Accounts”](#) section on page 15-18.
- 

## Using the Cisco Unity Administrator to Create Individual Subscriber Accounts

By using the Cisco Unity Administrator, you can create a regular subscriber account by importing existing user data from Domino.

## Importing Existing User Data from the Message Store

You can use the Cisco Unity Administrator to create a subscriber account by importing a Person document from Domino. Within the Cisco Unity Administrator, you can select the person from the Domino address book, and Cisco Unity-specific attributes are written to the existing Person document when the subscriber is created. (You specify the address book that you want to use on the System > Configuration > Subscriber Address Books page in the Cisco Unity Administrator. See the “[Subscriber Address Book Settings](#)” section on page 28-7 for details.)

Note that when the Cisco Unity Bulk Import wizard creates a subscriber account, it does not:

- Import Windows domain account information for a person.
- Enable an Active Directory account if it is disabled.
- Create a Windows domain account for a person if one does not already exist.

This is important to note if subscribers will use Windows credentials to access the Cisco Unity Administrator and the Status Monitor. For more details, see the “[About Subscriber Accounts](#)” section on page 15-4.

You can use the following procedure to import existing user data from the Domino address book.

### To Create a Regular Subscriber Account by Importing Existing User Data

- 
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page.
- Step 2** Click the **Add** icon.
- Step 3** Click **Notes**.
- Step 4** In the Address Book list, confirm that the address book listed is the one that contains the user data that you want to import.
- If the address book that you want to use is not listed, go to the System > Configuration > Subscriber Address Books page and add a different address book (for details on how to add an address book, see the “[Subscriber Address Book Settings](#)” section on page 28-7).
- Step 5** In the Find Domino Person By list, indicate whether to search by short name, first name, or last name.
- Step 6** Enter the applicable short name or name. You also can enter \* to display a list of all users, or enter one or more characters followed by \* to narrow your search.
- Step 7** Click **Find**.
- Step 8** On the list of matches, click the name of the user to import.
- Step 9** On the Add Subscriber page, enter the applicable information.
- Step 10** Click **Add**.
- Step 11** On the subscriber record, customize settings as applicable, and then click the **Save** icon.
- 

Use the following table to learn more about the settings on the Add Subscriber page.

**Table 15-3 Add Subscriber Page**

Field	Considerations
First Name/Last Name	<i>Display only.</i> The first and last names of the subscriber. These fields are filled in automatically from the Person document.

Table 15-3 Add Subscriber Page (continued)

Field	Considerations
Display Name	<i>Display only.</i> This is the subscriber name as displayed in the Cisco Unity Administrator and subscriber reports. In most cases, only the first 40 characters are displayed.  This field is filled in automatically from the Person document.
Extension	Enter the number that callers dial to reach the subscriber. Enter numerals only, according to the extension numbering plan for your organization. The number must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one. However, a subscriber extension can be the same number as the subscriber Fax ID. Note that many phone system integration features, such as MWI and call forward to personal greeting, require that the Cisco Unity number plan match that of the phone system.  Enter any combination of digits from 0 to 9, up to a maximum of 40 digits.
Fax ID	Enter the number that callers dial to send a fax to the subscriber. This number may be the same as the subscriber extension.
Template	Select the template on which to base the subscriber account. The template affects most subscriber settings.
Short Name	<i>Display only.</i> The short name specified in the Domino Person document for the subscriber.
Server	The Domino server associated with the address book that you selected during import.
SMTP address (for Internet subscribers only)	Enter the e-mail (SMTP) address assigned to the Internet subscriber. Specify the e-mail (SMTP) address to which messages to the Internet subscriber will be sent:  SMTP:alias@domain.com (e.g. aabade@cisco.com)  Internet subscribers do not have Notes specified as their mail system in their Domino Person documents. The address maps to the Forwarding Address on the Person document for the subscriber. Instead, messages for the subscriber are sent to this e-mail address.

## After Creating Subscriber Accounts

After creating subscriber accounts, consider the following:

- If a subscriber account that you created has a disabled Active Directory account or does not have a Windows domain account, and will require Windows credentials to access the Cisco Unity Administrator or the Status Monitor, use GrantUnityAccess to associate the subscriber account with a Windows domain account. For details, see the [“About Subscriber Accounts” section on page 15-4](#). To use GrantUnityAccess, see the [“About the Accounts That Can Be Used to Administer Cisco Unity” section on page 2-11](#).
- Add individual subscribers to public distribution lists, as needed. For example, assign subscribers to screen those messages left in Cisco Unity that are not associated with a specific recipient, such as those left to the Unaddressed Messages distribution list or for the Opening Greeting call handler. See the [“Message Handling” section on page 6-2](#).
- Set up the client applications that subscribers will use to access Cisco Unity from their computers. For details on setting up subscribers to use the Cisco PCA, the Cisco Unity Assistant, and Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity, see the [“Setting Up Client Applications” chapter](#).
- Train new subscribers and operators to use Cisco Unity. See the [“Subscriber, Operator, and Support Desk Orientation” chapter](#) for a task list you can use to acquaint subscribers with Cisco Unity.

- When a subscriber leaves the organization or otherwise no longer needs a Cisco Unity account, you can delete the subscriber account. See the “[Deleting Subscriber Accounts](#)” chapter for details.

There are several ways to modify existing subscriber accounts. You can:

- Customize subscriber settings for individual accounts in the Cisco Unity Administrator (see the “[Subscriber Settings](#)” chapter for details).
- Use Bulk Edit to modify a subscriber setting shared by multiple subscriber accounts. For example, you might use this tool to change a setting so that a group of subscribers will no longer be listed in the phone directory, or you can associate a group of subscribers with a particular class of service. The Bulk Edit utility is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop.)
- (Re)run the Cisco Unity Bulk Import wizard to modify unique subscriber settings—such as primary or alternate extensions—for multiple subscribers at once. To do so, refer to the Cisco Unity Bulk Import wizard online Help.

Note that subscribers can also customize some of their own settings either by accessing the Cisco Unity Assistant or by using the subscriber phone conversation.





## Deleting Subscriber Accounts

---

Before deleting a subscriber account, review the information in this chapter. For information on deleting Internet subscribers, refer to the “Deleting Internet Subscribers” section in the “Internet Subscribers” chapter in the *Networking in Cisco Unity Guide*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/net/net403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net403/dom/index.htm).

### How to Delete a Subscriber Account

When a subscriber leaves the organization or otherwise no longer needs a Cisco Unity account, delete the account in the Cisco Unity Administrator. It is important that you delete the subscriber account in the Cisco Unity Administrator before you delete associated accounts in Windows and Domino, so that Cisco Unity can do the following tasks:

- Delete the subscriber from other Cisco Unity accounts, handlers, or call routing rules that send calls to the subscriber.
- Prompt you to reassign to another subscriber any call handlers that the subscriber owned or was the message recipient of.
- Prompt you to reassign to another subscriber any public distribution lists that the subscriber owned, and to remove the subscriber from all public distribution lists.

When you delete a subscriber who was assigned to review the messages sent to any of the following Cisco Unity entities, make sure that you assign another subscriber or a public distribution list to replace the deleted subscriber; otherwise, messages may be “lost.”

- Unaddressed Messages distribution list
- System Event Messages distribution list (because the Example Administrator is the only member of this distribution list by default)
- Operator call handler (because the Example Administrator is the only member of this distribution list by default)
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

To identify call handlers that are associated with improperly deleted accounts, run the Unresolved References report. See the “[Unresolved References Report](#)” section on page 26-11 for more information.

Use the following procedure to delete a subscriber account in the Cisco Unity Administrator.

#### To Delete a Subscriber Account

---

- Step 1** From any subscriber page, click the **Delete** icon.
- Step 2** Click **Delete**.
- 

## What Happens When a Regular Subscriber Account Is Deleted

When you delete a Cisco Unity subscriber account, Cisco Unity removes all data associated with the subscriber account from a SQL database on the Cisco Unity server.

In addition, Cisco Unity removes the small subset of subscriber account information that is stored in the Domino address book.

Note that deleting the Cisco Unity account does not delete the Windows domain account (if there is one) or the Domino Person document for that subscriber. As needed, the Windows domain account can be deleted separately after the subscriber account is deleted in the Cisco Unity Administrator.



# Subscriber Settings

---

## Overview: Subscriber Settings

When a subscriber account is created, it contains the settings defined in the subscriber template upon which it is based. You can customize these default settings by changing individual subscriber pages. See the following sections in this chapter for more information about making changes on individual subscriber pages.

- [Subscriber Profile Settings, page 17-2](#)
- [Subscriber Account Settings, page 17-4](#)
- [Subscriber Phone Password Settings, page 17-5](#)
- [Subscriber Private List Settings, page 17-6](#)
- [Subscriber Conversation Settings, page 17-7](#)
- [Subscriber Call Transfer Settings, page 17-11](#)
- [Subscriber Greetings Settings, page 17-13](#)
- [Subscriber Caller Input Settings, page 17-16](#)
- [Subscriber Messages Settings, page 17-17](#)
- [Subscriber Message Notification Settings, page 17-20](#)
- [Subscriber Alternate Extension Settings, page 17-25](#)

### Changing Settings for Multiple Subscribers at Once

If you want to change settings for multiple subscribers at once, there are two methods for you to choose from:

- Use the Bulk Edit utility to modify a subscriber setting shared by multiple subscriber accounts. For example, you might use this tool to change a setting so that a group of subscribers will no longer be listed in the phone directory, or you can associate a group of subscribers with a particular class of service. Bulk Edit is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop.)
- (Re)run the Cisco Unity Bulk Import wizard when you want to modify unique subscriber settings—such as phone passwords or extensions—for multiple subscribers at once. To do so, refer to the Cisco Unity Bulk Import wizard online Help. (To access the Cisco Unity Bulk Import wizard, on the Windows Start menu, click Programs > Cisco Unity > Cisco Unity Bulk Import.)

Note that some of the settings that you enter on the subscriber pages of the Cisco Unity Administrator can also be changed by subscribers. Subscribers can customize some of their own settings either by accessing the Cisco Unity Assistant or by using the subscriber phone conversation. (In version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

## Subscriber Profile Settings

Profile settings define how Cisco Unity identifies a subscriber. Some of these settings are defined in the subscriber template, but most are defined in the Cisco Unity account for each individual subscriber.

Use the following table to learn more about subscriber profile settings.

**Table 17-1** *Subscribers > Subscribers > Profile Page*

Field	Considerations
First Name/Last Name	<p><i>Display only.</i> The first and last names of the subscriber. These fields are filled in automatically from the Person document.</p> <p>The names entered here are used for directory assistance. Note that subscribers must also have recorded names to be listed in the phone directory.</p>
Display Name	<p><i>Display only.</i> This setting shows the subscriber name as displayed in the Person document and in the Cisco Unity Administrator. This field is filled in automatically from the Person document.</p> <p>In most cases, only the first 40 characters are displayed.</p>
Class of Service	<p>Select the class of service to which the subscriber is assigned. The class of service defines permissions and restrictions for using Cisco Unity. To view the details of the selected class of service, click the View link. Note that when you click the link, you leave the Subscribers &gt; Subscribers &gt; Profile page, and move to the Subscribers &gt; Class of Service &gt; Profile page.</p>
Extension	<p>Enter the number that callers dial to reach the subscriber. Enter numerals only, according to the extension numbering plan for your organization. The number must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one. However, a subscriber extension can be the same number as the subscriber Fax ID. Note that many phone system integration features, such as MWI and call forward to personal greeting, require that the Cisco Unity number plan match that of the phone system.</p> <p>Enter any combination of digits from 0 to 9, up to a maximum of 40 digits.</p>
Fax ID	<p>Enter the number that callers dial to send a fax to the subscriber. This number may be the same as the subscriber extension.</p> <p>Enter the number that callers dial to send a fax to the subscriber.</p>
Fax Delivery Number	<p>Enter the number that Cisco Unity uses to deliver a fax message to a fax machine. The Fax Delivery Number field appears only if the subscriber belongs to a class of service that permits access to FaxMail.</p>
Recorded Voice	<p>This is the recorded name of the subscriber. You can record a name here for the subscriber, or the subscriber can record the name by using the self-enrollment conversation, the setup options, or by using the Cisco Unity Assistant.</p> <p>To record the subscriber name here, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.</p>

Table 17-1 Subscribers &gt; Subscribers &gt; Profile Page (continued)

Field	Considerations
Active Schedule	Select a schedule to specify the days and times that the standard and closed subscriber greetings play, as well as the action that Cisco Unity takes after the greeting. To view details of the selected schedule, click the View link. Note that when you click the link, you leave the Profile page, and move to the System > Schedules page.
Time Zone	Select the desired time zone for the subscriber. The default time zone setting is Default, which is the time zone set on the Cisco Unity server. Change this setting only for those subscribers who are located in a different time zone than the Cisco Unity server. The subscriber time zone setting is used for: <ul style="list-style-type: none"> <li>The Message Received Time—When a subscriber listens to messages over the phone, Cisco Unity announces the time that a message was received by using the local time specified for the subscriber.</li> <li>The Message Notification Schedule—The schedule displayed on the subscriber Message Notification page and in the Cisco Unity Assistant uses the local time specified for the subscriber.</li> </ul> Note that even if you change the time zone setting for a subscriber, the time zone setting on the Cisco Unity server is used to determine when standard and closed greetings are played for callers.
Switch (for dual phone system integrations only)	Select the phone system that the subscriber uses. If this setting is incorrect, Cisco Unity will not be able to: <ul style="list-style-type: none"> <li>Transfer calls to or from the subscriber.</li> <li>Turn message waiting indicators (MWIs) on or off.</li> <li>Dial the subscriber extension when the phone is selected as the recording and playback device for the Media Master.</li> </ul> On the System > Ports page, the selected phone system must have an appropriate number of ports set to answer calls and to dial out for MWIs and Media Master recording and playback by phone.
Set Subscriber for Self-Enrollment at Next Login	Check this check box so that the subscriber will be asked at the next logon to record a name and a standard greeting, to set a password, and to choose whether to be listed in directory assistance. Once the subscriber has enrolled, the check box is unchecked automatically. This setting is most commonly used for new subscribers.
List in Phone Directory	Check this check box to list the subscriber in directory assistance, which callers can use to reach subscribers. In addition to checking this check box, note that subscribers must also have recorded names to be listed in the phone directory. When allowed by the class of service, subscribers can change this setting over the phone or by using the Cisco Unity Assistant.
Phone Security Level	<i>Display only.</i> This setting indicates whether the subscriber belongs to a class of service (COS) that uses regular or enhanced phone security. Regular security indicates that the subscriber uses a password when logging on to Cisco Unity. Enhanced security indicates that the subscriber account uses RSA two-factor user authentication. You select the phone security level for a COS on the Subscribers > Class of Service > Profile page.
Enhanced Security User Alias	Enter the subscriber RSA alias, if you are using enhanced phone security. If this field is left blank, Cisco Unity uses the Domino short name as the RSA alias for the subscriber. The RSA alias that Cisco Unity uses for the subscriber must match the RSA alias that is in the corresponding user account on the ACE/Server. If you change the RSA alias here, you must also change it on the ACE/Server by using the Database Administrator program.
Short Name	<i>Display only.</i> The short name specified in the Domino Person document for the subscriber.
Server	<i>Display only.</i> The Domino server associated with the address book that you selected during import.

Table 17-1 Subscribers &gt; Subscribers &gt; Profile Page (continued)

Field	Considerations
Database Filename	<i>Display only.</i> The mail file specified on the Mail tab of the Domino Person document for the subscriber.
User Name	<i>Display only.</i> The hierarchical name specified on the Basics tab in the Domino Person document for the subscriber.
SMTP Address (for Internet subscribers only)	Enter the e-mail (SMTP) address assigned to the Internet subscriber. Specify the e-mail (SMTP) address to which messages to the Internet subscriber will be sent:  SMTP:alias@domain.com (for example, aabade@cisco.com)  Internet subscribers do not have Notes specified as their mail system in their Domino Person documents (the address maps to the Forwarding Address on the Person document for the subscriber.) Instead, messages for the subscriber are sent to this e-mail address.

## Subscriber Account Settings

You can use the account settings to check the account status for an individual subscriber (whether an account is locked or unlocked). Cisco Unity locks a subscriber account automatically when the Cisco Unity Account Status check box is checked on the Subscribers > Subscriber Template > Account for the template that was used to create the subscriber account.

Cisco Unity also locks a subscriber account when the subscriber reaches the limit of failed logon attempts specified in the account policy:

- When subscribers use the phone to access Cisco Unity, the number of failed logon attempts allowed is set on the Subscribers > Account Policy > Unity Account Lockout page.
- When subscribers use the Cisco Personal Communications Assistant (PCA) to access Cisco Unity, the number of failed logon attempts allowed is set on the System > Configuration > Authentication Provider page.
- When subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity, and the applications use the Integrated Windows authentication method (which is the default), the account policy that is specified for each Windows domain account determines the number of failed logon attempts that Windows allows before the user account cannot be used to access Windows (and therefore, the Cisco Unity Administrator or the Status Monitor).

However, when subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity, and the applications use the Anonymous authentication method, the number of failed logon attempts allowed is set on the System > Configuration > Authentication Provider page.

You can use the account settings to lockout individual subscriber accounts to prevent subscribers from using the phone or a Cisco Unity web application to access Cisco Unity, or to specify billing IDs specific to your organization.

Note that you cannot use the account settings to change the logon, password, or lockout policy for individual subscriber accounts. To customize an account policy for all Cisco Unity subscribers, see the [“Authentication Settings” section on page 28-11](#). For information on setting up the account policy that applies when subscribers access to Cisco Unity by phone, see the [“Account Policy Settings” chapter](#).

Use the following table to learn more about subscriber account settings.

**Table 17-2** *Subscribers > Subscribers > Account Page*

Field	Considerations
Cisco Unity Account Status	Check this check box to lock the account; uncheck it to unlock the subscriber account. When an account is locked, the subscriber cannot access Cisco Unity by phone, but the subscriber can use the Cisco Unity Administrator, Status Monitor, Cisco Personal Communications Assistant (PCA), and Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.
Cisco Unity GUI Access Status	Check this check box to lock an account; uncheck it to unlock the subscriber account. When a subscriber account is locked, the subscriber cannot access Cisco Unity by using the Cisco Unity Administrator, Status Monitor, or the Cisco Personal Communications Assistant (PCA), but the subscriber can access it by phone or by using the Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.  This field does not lock or unlock Windows domain accounts.
Created	<i>Display only.</i> This setting shows the date and time that the subscriber account was created.
Last Phone Contact	<i>Display only.</i> This setting shows the date and time that the subscriber last accessed the account by phone.
Billing ID	Enter organization-specific information, such as accounting information, department names, or project codes. This information can be included in subscriber reports.
Call Handlers Owned	<i>Display only.</i> This setting shows call handlers that the subscriber owns. To view them, click the link on the handler name. Note that when you click the call handler link, you leave this page, and move to the Call Management > Call Handlers > Profile page.

## Subscriber Phone Password Settings

Phone password settings define whether subscribers can set their own phone passwords and when they must change their passwords. In addition, you can use the phone passwords for individual subscribers in the following situations:

- When a subscriber forgets a password, you can reset the password.
- When more than one subscriber has access to the same account, you can set the password and not allow subscribers to change it.

You can use the Cisco Unity Bulk Import wizard to set phone passwords for multiple subscriber accounts at the same time. (Refer to the Cisco Unity Bulk Import online Help for details.) As a best practice, specify a long—eight or more digits—and non-trivial password when you set subscriber passwords, and if you allow subscribers to change their own passwords, encourage them to do the same. (The minimum phone password length is specified on the Subscribers > Account Policy > Phone Password Restrictions page).

Note that the phone password is separate from any password a subscriber uses to log on to the operating system or to a Cisco Unity web application, such as the Cisco Unity Administrator or the Cisco Personal Communications Assistant (PCA). For information on the password settings that govern subscriber access to the Cisco Unity Administrator or the Cisco PCA, see the [“Authentication Settings” section on page 28-11](#).

Use the following table to learn more about subscriber password settings.

**Table 17-3** *Subscribers > Subscribers > Phone Password Page*

Field	Considerations
User Cannot Change Password	<p>Check this check box to prevent the subscriber from changing the phone password. Use of this setting is most applicable for accounts that can be accessed by more than one person. When you check this check box, also check the Password Never Expires check box.</p> <p>If you leave this check box unchecked, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Encourage them to specify long—eight or more digits—and non-trivial passwords as a way to protect their accounts from unauthorized access. (The minimum phone password length is specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page).</p>
User Must Change Password at Next Login	<p>Check this check box when you have set a temporary phone password, and want the subscriber to set a new password the next time that the subscriber logs on to Cisco Unity by phone.</p> <p>Encourage subscribers to specify long—eight or more digits—and non-trivial passwords as a way to protect their accounts from unauthorized access. (The minimum phone password length is specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page).</p>
Password Never Expires	<p>Check this check box for low-security subscribers or for accounts that can be accessed by more than one person.</p> <p>Uncheck the check box to require the subscriber to change the phone password at the interval specified on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page.</p>
Password	<p>Enter a password by using digits 0 through 9. To protect Cisco Unity from unauthorized access, enter a long—eight or more digits—and non-trivial password. (The minimum length of the password is set on the Subscribers &gt; Account Policy &gt; Phone Password Restrictions page.)</p> <p>To have Cisco Unity prompt the subscriber to set a new password, also check the User Must Change Password at Next Login check box.</p>
Confirm Password	Enter the new password again to confirm the entry.
Date of Last Change	<i>Display only.</i> This setting shows the date the password was last changed.

## Subscriber Private List Settings

Private distribution lists, like public distribution lists, are used to send voice messages to more than one subscriber at a time. You can set up private lists for a subscriber in the Cisco Unity Administrator, though the subscriber is the only person who can send voice messages to the list. Subscribers can set up private lists by using the Cisco Unity Assistant or by phone. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.) Refer subscribers to the “Changing Private List Settings” chapter in the *Cisco Unity User Guide* for details.

Note that private distribution lists in Cisco Unity are stored on the server with the other subscriber settings. Therefore, subscribers can address messages to private lists only over the phone, not from Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.

For detailed instructions, refer subscribers to the “Sending and Responding to Messages” chapter of the *Cisco Unity User Guide*. (The *Cisco Unity User Guide* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/ug/ug403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/ug/ug403/dom/index.htm).)

Use the following table to learn more about subscriber private list settings.

**Table 17-4** *Subscribers > Subscribers > Private Lists Page*

Field	Considerations
Private Lists	Select the list to which the settings on the rest of the page will apply. You can modify the settings on this page for the selected list. To create a new list, click an empty list and add settings, or click a list that is no longer used and modify the settings.
Name of List	This setting shows the name of the selected list.
Recorded Name	This is the recorded name of the list. Because subscribers address messages to private lists by phone only in number mode, Cisco Unity plays the recorded name so that subscribers can verify if they have addressed the message to the correct list.  To record a list name, use the Media Master control bar. Use the Paste From File option on the Options menu to use a prerecorded WAV file. Note that the Media Master is not available across a firewall.
Current Members of <List>	This setting shows the subscribers on the list. There is no limit imposed on the number of subscribers that can be added to a private list. Other private lists cannot be members of a private list; however, a public distribution list can be a member of a private list. To add or remove subscribers from the list, click Change Members.

## Subscriber Conversation Settings

The Cisco Unity conversation—or the TUI (telephone user interface)—is a set of prerecorded instructions and options that Cisco Unity plays over the phone to subscribers when they listen to, send, and manage messages, and when they change their Cisco Unity settings. Conversation settings define some of what subscribers hear and how they hear it.

Some of the customizations that you can make by using the conversation settings include:

- Setting volume level, and selecting the language in which Cisco Unity plays instructions to the subscriber.
- Specifying which conversation style subscribers hear. You can also specify whether subscribers hear the comprehensive instructions offered by the full menus or brief menus for each conversation style. (For information on using Optional Conversation 1 rather than the standard conversation style, see the [“Activating Optional Conversation 1 for Subscribers”](#) section on page 7-3.)
- Enabling Cisco Unity to play a prompt that reminds subscribers when their alternate greeting is turned on.
- Determining whether subscribers address messages to other subscribers by entering extensions, by spelling first names, or by spelling last names.
- Dictating how messages are presented to subscribers over the phone. For example, you can specify whether subscribers hear the Message Type menu, message counts, and timestamps when they check messages, and you can specify the order in which Cisco Unity plays messages.
- Selecting the destination—such as a call handler, interview handler, subscriber, or directory assistance—that Cisco Unity sends subscribers to when they exit the subscriber conversation.

Use the following table to learn more about subscriber conversation settings. To learn more about additional ways that you and subscribers can change the conversation, see the [“How You Can Customize the Conversation”](#) section on page 7-1 and the [“How Subscribers Can Customize the Cisco Unity Conversation”](#) section on page 7-9.

**Table 17-5** *Subscribers > Subscriber > Conversation Page*

Field	Considerations
Menu Style	<p>Choose one of these options:</p> <ul style="list-style-type: none"> <li>• Full Menus—Subscribers hear comprehensive instructions; select for a new subscriber.</li> <li>• Brief Menus—Subscribers hear abbreviated versions of the full menus; select for a more experienced subscriber.</li> </ul>
Volume Level <i>(for analog or DTMF integrations only)</i>	Select the volume level at which subscribers hear the Cisco Unity conversation. Subscribers can also adjust the volume temporarily from their phones.
Language	<p>Select the language in which the subscriber conversation plays instructions to subscribers.</p> <p>The language setting also controls the language used for Text to Speech (TTS). (Note that to use TTS, your organization must purchase TTS licenses and install the applicable TTS languages. TTS is controlled by class of service.)</p> <p>The TTY language allows TTY subscribers to read Cisco Unity prompts and to record messages by using a TTY device. TTY functionality is supported only when G.711 is selected as the system-wide message recording and storage codec.</p>
Time Format	<p>Select the time format used for the message timestamps that subscribers hear when they listen to their messages over the phone:</p> <ul style="list-style-type: none"> <li>• System Default—Subscribers hear message timestamps in the time format specified in the Use 24-Hour Time Format for Conversation and Schedules field on the System &gt; Configuration &gt; Settings page.</li> <li>• 12-Hour Clock—Subscribers hear 1:00 PM when listening to the timestamp for a message left at 1:00 PM.</li> <li>• 24-Hour Clock—Subscribers hear 13:00 when listening to the timestamp for a message left at 1:00 PM.</li> </ul> <p>Subscribers can set their own time format preferences in the Cisco Unity Assistant.</p>
Conversation Style	<p>Select the conversation style that subscribers hear when they listen to and manage their messages over the phone:</p> <ul style="list-style-type: none"> <li>• Standard Conversation—Subscribers hear the menus depicted in the <i>Cisco Unity Phone Menus for the Standard Conversation</i>.</li> <li>• Optional Conversation 1—Subscribers hear the menus depicted in the <i>Cisco Unity Phone Menus for Optional Conversation 1</i>.</li> </ul> <p>You can use either full or brief menu style with each conversation style.</p>

Table 17-5 Subscribers &gt; Subscriber &gt; Conversation Page (continued)

Field	Considerations
When Exiting the Conversation, Send Subscriber To	<p>Select the destination to which Cisco Unity sends the subscriber when exiting the conversation.</p> <ul style="list-style-type: none"> <li>• Call Handler—Sends the call to the call handler that you select.</li> <li>• Directory Handler—Sends the call to directory assistance.</li> <li>• Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>• Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>• Interview Handler—Sends the call to the interview handler that you select.</li> <li>• CVM Mailbox Reset—Sends the call to the mailbox reset conversation. (Available only when you use the Community Voice Mail package.)</li> <li>• Sign-In—Sends the call to the subscriber logon conversation.</li> <li>• Subscriber—Sends the call to the subscriber that you select.</li> </ul>
Identify a Subscriber By	<p>Select how the conversation prompts subscribers to address messages to other subscribers. Subscribers can address messages over the phone by entering subscriber extensions, by spelling their first names, or by spelling their last names. Addressing by name requires lettered keypads on subscriber phones.</p> <p>Regardless of the option you choose here, as subscribers address a message by phone, they can switch between addressing by name and addressing by extension by pressing the # key twice. However, when the Enable Spelled Name Search check box is unchecked on the System &gt; Configuration &gt; Settings page, subscribers can address messages over the phone only by entering subscriber extensions.</p>
Subscriber Recorded Name	<p>Check this check box to have Cisco Unity play the recorded name of the subscriber when the subscriber accesses Cisco Unity by phone.</p> <p>Uncheck the check box to have Cisco Unity go directly to the message count.</p>
Alternate Greeting Notification	<p>Check this check box to have Cisco Unity notify subscribers when they have their alternate greeting turned on.</p> <p>Cisco Unity plays the notification immediately after subscribers log on to Cisco Unity by phone, and then Cisco Unity plays a menu from which subscribers can choose to leave their alternate greeting on, turn it off, or play it.</p>
Message Count Totals	<p>Check this check box to have Cisco Unity announce the total number of messages that are marked new. The number includes voice, e-mail, fax, and receipt messages, as applicable.</p>
Voice Message Count	<p>Check this check box to have Cisco Unity announce the number of voice messages that are marked new.</p>
E-Mail Message Count	<p>Check this check box to have Cisco Unity announce the number of e-mail messages that are marked new.</p>
Fax Count	<p>Check this check box to have Cisco Unity announce the number of fax messages that are marked new.</p>
Saved Message Count	<p>Check this check box to have Cisco Unity announce the total number of messages that have been saved. The number includes voice, e-mail, fax, and receipt messages.</p>

Table 17-5 Subscribers &gt; Subscriber &gt; Conversation Page (continued)

Field	Considerations
Message Type Menu	<p>Check this check box so that Cisco Unity plays the following menu when subscribers log on to Cisco Unity over the phone:</p> <ul style="list-style-type: none"> <li>• Press 1 to hear voice messages</li> <li>• Press 2 to hear e-mails</li> <li>• Press 3 to hear faxes</li> <li>• Press 4 to hear receipts</li> </ul> <p>Note that although the e-mail and fax options are available in the Message Type Menu, Cisco Unity plays e-mails and faxes only when the subscriber is assigned to a class of service that has the Text to Speech (TTS) and FaxMail features enabled. With fax messages, Cisco Unity plays only message properties (for example, the sender, date, and time).</p> <p>Subscribers can also enable the Message Type menu by using the Cisco Unity Assistant.</p>
Sort by Message Type	<p>Select a message type, and then click the Move Up and Move Down buttons to reorder the list of message types. Cisco Unity plays messages in the order that you specify here.</p> <p>Cisco Unity plays e-mails and faxes only when the subscriber is assigned to a class of service that has the Text to Speech (TTS) and FaxMail features enabled. With fax messages, Cisco Unity plays only message properties (for example, the sender, date, and time).</p> <p>Subscribers can also specify the order in which Cisco Unity plays new and saved messages by using the Cisco Unity Assistant.</p>
Then By	<p>Click Newest First or Oldest First to specify the message order for new and saved messages.</p> <p>Note that except for receipts, urgent messages are always played before regular messages for each message type (receipts are sorted by the time that they were sent).</p>
Sender's Information	<p>Check this check box so that Cisco Unity plays caller information about a message sender before playing a message. The information that Cisco Unity plays depends on how Cisco Unity is set up.</p> <p>By default, Cisco Unity plays the following information when the Sender's Information check box is checked:</p> <ul style="list-style-type: none"> <li>• For messages left by an identified subscriber, Cisco Unity plays the recorded name of the subscriber before playing the message. If the subscriber does not have a recorded name, Cisco Unity plays the primary extension associated with the subscriber instead.</li> <li>• For messages left by an unidentified caller, Cisco Unity does not provide the phone number (ANI or caller ID) information before playing the message.</li> </ul> <p>However, you can use the Bulk Edit utility (available in Tools Depot) to enable Cisco Unity to announce additional caller information when the Sender's Information check box is checked:</p> <ul style="list-style-type: none"> <li>• For messages left by an identified subscriber, Cisco Unity plays the recorded name (if available) and the extension before playing the message.</li> <li>• For messages left by unidentified caller, Cisco Unity plays the phone number (if available) of the caller before playing the message.</li> </ul>
Message Number	<p>Check this check box to have Cisco Unity announce the sequential number of a message ("Message one...").</p> <p>Use with the Message Count Totals check box to help subscribers keep track of the number of unheard messages.</p>

**Table 17-5** *Subscribers > Subscriber > Conversation Page (continued)*

Field	Considerations
Before Playing Each Message, Play: Time the Message Was Sent	Check this check box to have Cisco Unity announce the date and time a message was sent, before playing the message.
After Playing Each Message, Play: Time the Message Was Sent	Check this check box to have Cisco Unity announce the date and time a message was sent, after playing the message.

## Subscriber Call Transfer Settings

Call transfer settings specify whether unidentified callers are transferred to a phone or to the greetings of a subscriber or handler. These settings also specify how Cisco Unity handles a transfer: Cisco Unity can either release the call to the phone system, or it can supervise the transfer.

When Cisco Unity is set to supervise transfers, it can provide additional call control with call holding and call screening:

- With call holding, when the phone is busy, Cisco Unity can ask callers to hold. Cisco Unity plays hold music, and approximately every 30 seconds, tells callers on hold how many callers are ahead of them and allows them to continue holding, leave a message, or try another extension. There is no limit to the number of callers that can be holding.

If call holding is not selected, callers are sent to whichever subscriber or handler greeting is enabled—either the busy, standard, closed, or alternate greeting.

- With call screening, Cisco Unity can ask for the name of the caller before connecting to a subscriber. The subscriber can then hear who is calling and, when a phone is shared by more than one subscriber, who the call is for. The subscriber can then accept or refuse the call.

Both primary and alternate extensions utilize the same transfer settings. Use the following table to learn more about subscriber call transfer settings.

**Table 17-6** *Subscribers > Subscribers > Call Transfer Page*

Field	Considerations
Transfer Incoming Calls to Subscriber's Phone	<p>Choose one of these options:</p> <ul style="list-style-type: none"> <li>• No (Send Directly)—The extension assigned to the subscriber does not ring for unidentified callers; Cisco Unity plays the subscriber greeting.</li> <li>• Yes, Ring Subscriber's Extension—Cisco Unity sends calls to the extension assigned to the subscriber (displayed in the adjacent box). When Supervise Transfer is selected, use in conjunction with Rings to Wait For field to set the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</li> <li>• Yes, Ring Subscriber at This Number—Cisco Unity sends calls to the number entered in the adjacent box. When Supervise Transfer is selected, use in conjunction with Rings to Wait For field to set the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</li> </ul> <p>Note that the restriction tables associated with your class of service—rather than the subscriber COS—may prohibit you from entering certain phone numbers for subscribers.</p>
Transfer Type	<p>Select how Cisco Unity transfers calls. Use this setting with caution and only if you understand its implications on the phone and voice messaging systems.</p> <ul style="list-style-type: none"> <li>• Release to Switch—Cisco Unity puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Cisco Unity—forwards the call to the subscriber or handler greeting. This transfer type allows Cisco Unity to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system.</li> <li>• Supervise Transfer—Cisco Unity acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Cisco Unity—not the phone system—forwards the call to the subscriber or handler greeting. You can use supervised transfer whether or not the phone system forwards calls.</li> </ul> <p>The Transfer Type option is unavailable when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Rings to Wait For	<p>Select the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</p> <p>Set this value to at least 3 to give subscribers a chance to answer. Avoid setting to more than 4, especially if the call may be transferred to another extension, where the caller might have to wait for another four rings. This value should be at least two rings fewer than the phone system setting for forwarding calls.</p> <p>This option is unavailable when Transfer Incoming Calls is set to the No (Send Directly) option and when Release to Switch is selected.</p>

Table 17-6 *Subscribers > Subscribers > Call Transfer Page (continued)*

Field	Considerations
If the Call Is Busy	<p>Select the action that Cisco Unity performs for unidentified callers when the subscriber phone is busy. You may want to use holding options sparingly, because having calls on hold can tie up ports.</p> <ul style="list-style-type: none"> <li>• Always Hold—Cisco Unity plays a prompt indicating that the extension is busy. The caller is put on hold.</li> <li>• No Holding—Cisco Unity prompts the caller to leave a message and allows the caller to dial another extension.</li> <li>• Ask Caller—Cisco Unity gives the caller the options of holding, leaving a message, or dialing another extension.</li> </ul> <p>These options are unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Announce	<p>Check this check box to have Cisco Unity say “transferring call” when the subscriber answers the phone, to indicate that the call is from an unidentified caller.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Introduce (Call for Name)	<p>Check this check box to have Cisco Unity say “call for &lt;subscriber recorded name&gt;” or “call for &lt;dialled extension number&gt;” when the subscriber answers the phone. This setting applies only to calls from unidentified callers. Use this setting when subscribers share a phone or a subscriber takes calls for more than one dialed extension.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Confirm (Call Can Be Accepted or Refused)	<p>Check this check box to have Cisco Unity prompt the subscriber to accept or refuse a call from an unidentified caller. If the call is accepted, it is transferred to the subscriber phone. If the call is refused, Cisco Unity plays the appropriate subscriber greeting. You use this setting with the Ask Caller’s Name setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>
Ask Caller’s Name	<p>Check this check box to have Cisco Unity prompt unidentified callers to say their names. When the phone is answered, the subscriber hears “Call from...” before Cisco Unity transfers the call. You use this setting with the Confirm setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p>

## Subscriber Greetings Settings

Each subscriber and call handler can have up to five greetings. The greeting settings specify which greetings are enabled and the actions that Cisco Unity takes during and after each greeting. Enabling a greeting makes it available for Cisco Unity to use in applicable situations.

The greeting that plays when a caller reaches a subscriber or call handler depends on:

- The active schedule.
- The greeting source.
- Whether the call is internal.

- Whether the called extension is busy.

Cisco Unity greetings for subscribers and call handlers are:

<b>Standard</b>	Plays at all times unless overridden by another greeting.
<b>Closed</b>	Plays during the closed (nonbusiness) hours defined for the active schedule. When in effect, the closed greeting overrides the standard greeting, and thus limits the standard greeting to the open hours defined for the active schedule.
<b>Internal</b>	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 and closed greetings. Not all phone system integrations provide the support necessary for an internal greeting.
<b>Busy</b>	Plays when the extension is busy. (For example, “All of our operators are with other customers.”) A busy greeting overrides the standard, closed, and internal greetings. Not all phone system integrations provide the support necessary for a busy greeting.
<b>Alternate</b>	<p>Can be used for a variety of special situations, such as vacations or a holiday. (For example, “I will be out of the office until...”)</p> <p>Neither you nor Cisco Unity subscribers can schedule in advance when or for how long an alternate greeting is enabled. When enabled, an alternate greeting plays until you or the subscriber disables it, and overrides all other greetings.</p> <p>You can enable Cisco Unity to notify subscribers when their alternate greeting is turned on, by changing a setting on the template and subscriber Conversation pages in the Cisco Unity Administrator.</p>

Subscribers can record and enable all of their greetings by phone, or by using the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

Use the following table to learn more about subscriber greeting settings.

**Table 17-7** *Subscribers > Subscribers > Greetings Page*

<b>Field</b>	<b>Considerations</b>
Greeting	Select the greeting that you want to specify settings for. This setting does not reflect which of the greetings is active.
Status	Indicate whether the selected greeting is enabled. When a greeting is enabled, Cisco Unity plays it in the applicable situation. Recording a greeting does not automatically enable it; it must be enabled here.

Table 17-7 *Subscribers > Subscribers > Greetings Page (continued)*

Field	Considerations
Source	<p>Indicate the source for the greeting selected in the Greeting field:</p> <ul style="list-style-type: none"> <li>• <b>System</b>—Select to use the prerecorded system default greeting. Cisco Unity plays a prerecorded greeting along with the recorded name of the subscriber (for example, “Sorry, &lt;subscriber name&gt; is not available”). If the subscriber does not have a recorded name, Cisco Unity plays the subscriber extension instead.</li> <li>• <b>Recording</b>—Select to use a personal recording for the subscriber (or call handler). To record and play greetings here, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.</li> <li>• <b>Blank</b>—Select to have no recording. When the greeting source is left blank, Cisco Unity immediately performs the after-greeting action.</li> </ul>
Allow Caller Input	<p>Check this check box to enable settings specified on the Caller Input page. These settings contain actions assigned to caller key presses during the greeting. (For example, “To speak to my assistant, press 3.”)</p> <p>Click the Caller Input link to view the Caller Input page. Note that when you click the link, you leave the Greetings page.</p>
After Greeting	<p>Indicate the action that Cisco Unity performs after the greeting plays:</p> <ul style="list-style-type: none"> <li>• <b>Take Message</b>—Cisco Unity records a message from the caller. Click the Take Message link to view the Messages page.</li> <li>• <b>Say Good-Bye</b>—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• <b>Send Caller To</b>—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– <b>Call Handler</b>—Sends the call to the call handler that you select.</li> <li>– <b>Directory Handler</b>—Sends the call to directory assistance.</li> <li>– <b>Greetings Administrator</b>—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– <b>Hang Up</b>—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– <b>Interview Handler</b>—Sends the call to the interview handler that you select.</li> <li>– <b>Sign-In</b>—Sends the call to the subscriber logon conversation.</li> <li>– <b>Subscriber</b>—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>
Reprompt the User After This Many Seconds of Silence	<p>Check this check box and enter a value in the field on the right to indicate the number of seconds of silence to allow. When Cisco Unity receives no input from a caller within this number of seconds, Cisco Unity prompts the caller again.</p>
Number of Times to Reprompt	<p>Indicate the number of times to reprompt a caller. After the number of times indicated here, Cisco Unity performs the after-greeting action.</p>

# Subscriber Caller Input Settings

Caller input settings define actions that Cisco Unity takes in response to touchtone keys pressed by callers. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page.

Caller input settings are available only in the Cisco Unity Administrator; however, the greeting that mentions the key presses can be recorded either by the subscriber or the administrator. (For example, “I am unable to take your call right now. To speak to my assistant, press 3. To leave a message, press 4. To speak to a sales representative, press 5.”)

Use the following table to learn more about subscriber caller input settings.

**Table 17-8** *Subscribers > Subscribers > Caller Input Page*

Field	Considerations
Allow Callers to Dial an Extension During Greeting	<p>Check this check box to allow callers to enter an extension while the greeting plays. Use in conjunction with the Lock This Key check box to allow callers to enter some extensions but not others.</p> <p>This option is unavailable if the Allow Caller Input check box is unchecked on the Greetings page.</p>
Milliseconds to Wait for Additional Digits	<p>Indicate the amount of time Cisco Unity waits for additional input after callers press a single key that is not locked. If there is no input within this time, Cisco Unity performs the action assigned to the single key.</p> <p>A value of 1500 (one and one-half seconds) is recommended.</p> <p>This option is unavailable if the Allow Callers to Dial an Extension During Greeting check box is unchecked.</p>
Lock This Key to the Action	<p>Check this check box to have Cisco Unity ignore additional input after callers press the key; Cisco Unity performs the action assigned to the key. To create efficient caller input menus, lock all keys except those that begin extensions on your system. You also can lock a key to block calls to extensions that begin with that key.</p> <p>To lock the actions for all keys, uncheck the Allow Callers to Dial an Extension During Greeting check box.</p>

Table 17-8 Subscribers &gt; Subscribers &gt; Caller Input Page (continued)

Field	Considerations
Action	<p>Indicate the action that Cisco Unity performs after a caller presses the corresponding key. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page.</p> <ul style="list-style-type: none"> <li>• Ignore Key—No action taken. Cisco Unity plays the entire greeting, then performs the after-greeting action.</li> <li>• Skip Greeting—Cisco Unity skips the greeting and performs the after-greeting action. Skip Greeting is assigned to # by default to provide callers a standard way to skip greetings.</li> <li>• Take Message—Cisco Unity records a message from the caller. The greeting should indicate that a message will be recorded. Click the Take Message link to view the associated Messages page.</li> <li>• Say Good-Bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>

## Subscriber Messages Settings

Message settings define the following:

- The maximum recording length for messages from unidentified callers. (Note that for some integrations, you can set up Cisco Unity so that as a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. See the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19.)
- What unidentified callers can do when leaving messages.
- The language of the Cisco Unity prompts that callers hear when leaving messages.
- Whether subscribers are notified with message waiting indicators (MWIs) that they have voice messages.
- One or more extensions where the MWI will be activated when subscribers have voice messages.

For information on how you can change the way that Cisco Unity handles messages when calls are disconnected while subscribers are in the process of sending, replying to, or forwarding a message, see the [“How Cisco Unity Handles Messages That Are Interrupted by Disconnected Calls”](#) section on page 6-4.

**To Enable MWIs**

Cisco Unity can use the MWI on the phone to alert the subscriber to new voice messages. MWIs are not used to indicate the receipt of new e-mail, fax, or return receipt messages.

- 
- Step 1** In the Cisco Unity Administrator, go to the applicable **Subscribers > Subscribers > Messages** page.
- Step 2** Confirm that the **Use MWI for Message Notification** check box is checked.
- Step 3** Click the **Add** button located beneath the MWI Extensions table to add a row to the table. By default, the first row in the table contains an “X” to indicate the primary extension assigned to a subscriber. If you want one more extension and do not need to activate the MWI on the primary extension, you can also modify the first row.
- Step 4** Enter the applicable extension in the **Extension** field of the table. MWIs are automatically enabled for all rows in the table. When entering characters in the MWI Extensions table, consider the following:
- Enter digits 0 through 9.
  - Do not use spaces, dashes, or parentheses.
  - Enter , (comma) to insert a one-second pause.
  - Enter # and \* to correspond to the # and \* keys on the phone.
- Step 5** Click the **Save** icon.
- Step 6** Repeat [Step 3](#) through [Step 5](#) as necessary.
- 

To modify or disable an MWI for an extension, do the following procedure.

**To Modify or Delete Alternate MWIs**

- 
- Step 1** In the Cisco Unity Administrator, go to the applicable **Subscribers > Subscribers > Messages** page.
- Step 2** Do either of the following:
- To modify an extension, change the extension in the MWI Extensions table as applicable.
  - To delete extensions, check the check boxes next to the rows that you want to delete in the MWI Extensions table, and then click the **Delete** button.
- Step 3** Click the **Save** icon.
- Step 4** Repeat [Step 2](#) through [Step 3](#) as necessary.
- 

Use the following table to learn more about subscriber message settings.

**Table 17-9** *Subscribers > Subscribers > Messages Page*

Field	Considerations
Maximum Message Length in Seconds	Set the recording length allowed for messages left by unidentified callers. Recipients may want to limit the length of messages from unidentified callers. Some departments, such as Customer Service, may want to permit much longer messages. If enabled, a warning tone will sound before the maximum message length is reached.

Table 17-9 Subscribers &gt; Subscribers &gt; Messages Page (continued)

Field	Considerations
After Message Action	<p>Indicate the action that Cisco Unity performs after an unidentified caller leaves a message:</p> <ul style="list-style-type: none"> <li>• Say Good-Bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-Bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul>
Callers Can Edit Messages	<p>Check this check box to allow callers to be prompted to listen to, add to, rerecord, or delete their messages.</p> <p>Balance giving callers the additional control of editing messages with having voice messaging ports tied up for the additional time.</p>
Mark Messages as Urgent	<p>Indicate the action that Cisco Unity will allow:</p> <ul style="list-style-type: none"> <li>• Always—All messages left by unidentified callers are marked urgent. This may be useful for Sales or Technical Support call handlers.</li> <li>• Never—Messages left by unidentified calls are never marked urgent.</li> <li>• Ask Caller for Their Preference—Cisco Unity asks unidentified callers whether to mark their messages urgent.</li> </ul> <p>Note that Cisco Unity plays new urgent messages before other messages.</p>
Language That Callers Hear	<p>Select the language in which system prompts are played to callers. The language setting affects system prompts such as “You may record your message at the tone.”</p> <p>If you choose Inherited, Cisco Unity determines the language to use for system prompts on a per-call basis, depending upon the language set by the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.</p> <p>The default phone language and the list of languages shown here are set on the System &gt; Configuration &gt; Phone Languages page.</p>
Use MWI for Message Notification	<p>Check this check box to have Cisco Unity use the message waiting indicator (MWI) on the phone to alert the subscriber of new voice messages. MWIs are not used to indicate new e-mail, fax, or receipt messages.</p>
Indicator Lamps	<p><i>Display only.</i> Indicates whether the subscriber currently has any message waiting indicators (MWIs) on or off.</p>

Table 17-9 Subscribers &gt; Subscribers &gt; Messages Page (continued)

Field	Considerations
MWI Extensions	<p>When the Use MWI for Message Notification field is enabled, Cisco Unity uses the extension or extensions listed in the MWI Extensions table to activate message waiting indicators (MWIs).</p> <p>By default, one row in the table contains an “X” to indicate the primary extension assigned to a subscriber. You can change this row or add more rows to the table to have Cisco Unity activate MWIs for another extension or phone number. MWIs are enabled for all rows in the table; to disable an MWI for an extension, delete the row from the table.</p> <p>You can assign subscribers up to nine alternate MWIs. The alternate MWI extensions must be unique—up to the dialing domain level, if applicable—and no more than 30 digits in length</p> <p>When entering characters in the MWI Extensions table, consider the following:</p> <ul style="list-style-type: none"> <li>• Enter digits 0 through 9.</li> <li>• Do not use spaces, dashes, or parentheses between digits.</li> <li>• Enter , (comma) to insert a one-second pause.</li> <li>• Enter # and * to correspond to the # and * keys on the phone.</li> <li>• If the extension that you enter is intended to light an MWI on a phone that requires a different lamp code than the phone associated with the primary extension, make sure that your phone system is programmed to support multiple lamp codes.</li> <li>• MWIs are enabled for all rows in the table.</li> </ul>

## Subscriber Message Notification Settings

Cisco Unity can notify a subscriber of new messages by calling a phone or pager, or by sending an e-mail. Message notification settings allow you to control how and when Cisco Unity notifies a subscriber of new messages. You can set up notification for subscribers by using the Cisco Unity Administrator, and subscribers can set it up themselves by using the Cisco Unity Assistant, if available. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.) Subscribers can also enter the phone number and status of four of the notification devices—home phone, work phone, spare phone, and pager—by using the subscriber phone conversation.

To set up message notification, you select a notification device—phone, pager, or text pager—and enter a phone number or e-mail address, as applicable. The settings for each device allow you to control when and how notifications are sent to the first and subsequent devices. Generally, you adjust message notification settings on the message notification page of a specific subscriber and not in the subscriber template. However, you may want to enter notification settings in the subscriber template if, for example, you want to set up “chaining” or “cascading” message notification for an entire department of new subscribers. For more information, see the [“Chaining Message Notification”](#) section on page 17-21, and the [“Cascading Message Notification”](#) section on page 17-21.

Additionally, Cisco Unity can send message notifications in the form of text messages to text pagers, text-compatible cell phones, and e-mail addresses. For more information, see the [“Text Message Notifications”](#) section on page 17-22.

Use [Table 17-10](#) to learn more about subscriber message notification settings. Note that any message notification that you set up on the Subscribers > Subscribers > Message Notification Page is in addition to the message waiting indication that you set up on the Subscribers > Subscribers > Messages page. To set up message notification for a subscriber template, see the [“Subscriber Template Message Notification Settings”](#) section on page 13-17.

## Chaining Message Notification

Message notification can be set to “chain” to a series of notification devices if an attempt to send notification to the first selected device fails. The definition of failure to a notification device is based on the options you select for retrying a device that is not answered or is busy.

The Cisco Unity Administrator does not allow pager devices to be used for chaining message notification because notification to these devices does not fail.

### To Set Up Chaining Message Notification

---

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page.
  - Step 2** Click a notification device from the Device list, and enter settings for it, as applicable.
  - Step 3** Click another device in the If Notification Fails, Send Notification To field.
  - Step 4** In the Device list at the top of the page, click the same device that you indicated in [Step 3](#), and enter settings for it as you would normally, with the following exceptions:
    - In the Notify Subscriber Of table, uncheck all types and urgency of messages that should generate notification. If any message types are checked in this table, message notification for this device will commence immediately and will not wait for the notification failure of the previous device. Therefore, your notifications will not chain but all trigger at once.
    - In the Send Initial Notification After How Many Minutes field, leave the default setting of **0**.
  - Step 5** Repeat [Step 3](#) and [Step 4](#) for any subsequent devices that you wish to chain for message notification.
- 

## Cascading Message Notification

Cascading message notification allows you to set up a series of notifications to a widening circle of recipients.

For example, to create a hierarchy of message notifications for your Technical Support department, set the first message notification to be sent immediately to the pager of the front-line technical support representative. The next notification can be sent after a delay of 15 minutes to the pager of the department manager. A third notification can be sent after a delay of 30 minutes to an employee in the Problem Resolution Group.

Notifications continue to cascade according to the options you selected until the message has been saved or deleted by a recipient.

### To Set Up Cascading Message Notification

---

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page.
- Step 2** Select a notification device and enter settings for it, as applicable.
- Step 3** Specify the desired delay in the Send Initial Notification After How Many Minutes field. Typically, you will space notifications between the devices at regular intervals, such as every 15 minutes. For example, you might specify **0** as the delay for the first device, **15** as the delay for the second device, **30** for the third device, and so on.
- Step 4** Select **None** in the If Notification Fails, Send Notification To field.

**Step 5** Repeat [Step 2](#) through [Step 4](#) for the second and subsequent devices.

## Text Message Notifications

Cisco Unity can send message notifications in the form of text messages to text pagers, text-compatible cell phones, and e-mail addresses. When a message arrives that matches the criteria selected in the message notification settings, the Cisco Unity Messaging System sends a text message entered by you or the subscriber, such as “Urgent message for Technical Support.”

Note that to send text message notifications to text pagers, cell phones, or e-mail addresses, a site must have an SMTP gateway. If a site without an SMTP gateway attempts to deliver text message notifications, the notification attempt fails and a non-delivery receipt is sent to the Cisco Unity Messaging System and then routed, by default, to the Unaddressed Messages distribution list. (For more information, see the [“How Cisco Unity Handles Messages Without a Specific Recipient”](#) section on [page 6-3](#).)

Use the following table to learn more about subscriber message notification settings.

**Table 17-10** *Subscribers > Subscribers > Message Notification Page*

Field	Considerations
Device	Select the device that you want to use for message notification.
Phone Number <i>(not available for text pager notifications)</i>	<p>Enter the phone number, including trunk access code, of the selected device. Use digits 0 through 9 and the following dialing characters in the phone number:</p> <ul style="list-style-type: none"> <li>• , (comma) to insert a one-second pause.</li> <li>• # and * to correspond to the # and * keys on the phone.</li> </ul> <p>Subscribers can change this number over the phone.</p> <p>Note that the restriction tables associated with your class of service—rather than the subscriber COS—may prohibit you from entering certain phone numbers for subscribers.</p>
Extra Digits <i>(not available for text pager notifications)</i>	Enter any extra digits that Cisco Unity will dial after the phone number. The effect of the extra digits depends on the selected device. For pagers, the extra digits are shown on the pager display.
Dialing Options <i>(not available for text pager notifications)</i>	<p>Select the dialing options:</p> <ul style="list-style-type: none"> <li>• Try to Detect Connection—Cisco Unity waits until detecting a connection to dial the digits in Extra Digits.</li> <li>• Seconds to Wait—Cisco Unity can wait a specified number of seconds before dialing the digits in Extra Digits. Use this option if the automatic call progress detection is not reliable. Examples of poor call progress detection include noisy phone lines and unusual ringing patterns.</li> </ul>
To: (E-Mail Address) <i>(available for text pager notifications only)</i>	<p>Enter the e-mail address of the subscriber text pager, text-compatible cell phone, or another e-mail account (such as a home e-mail address).</p> <p>Up to 128 characters can be entered in this field.</p>

**Table 17-10 Subscribers > Subscribers > Message Notification Page (continued)**

Field	Considerations
From: (Phone Number) <i>(available for text pager notifications only)</i>	<p>Enter a phone number in this field if the subscriber has a text-compatible cell phone and wants text pager notifications to include a return phone number. Typically, this field contains the number that the subscriber calls to check messages.</p> <p>The From phone number appears in the last line of any text pager notification. A subscriber can press the Return Call button on many text-compatible cell phones to dial the phone number. The cell phone must support automatic callback in order to use this feature.</p> <p>Up to 40 characters can be entered in this field.</p>
Send: <i>(for text pager notifications only)</i>	<p>Enter the text message that the subscriber wants to receive in a text pager notification. For example, you might enter “Urgent message for Technical Support” for a subscriber who is on call for the technical support department.</p> <p>Every time a message arrives that matches the criteria selected in the message notification settings, the Cisco Unity Messaging System sends this text message.</p> <p>Up to 64 characters can be entered in this field.</p>
Include Voice Mail, E-Mail, and Fax Message Counts <i>(available for text pager notifications only)</i>	<p>Check this check box if you want the text pager notification to include a count of each voice mail, e-mail, and fax message.</p> <p>When the subscriber receives the notification, the message count appears as a line for each type of message. For example:</p> <ul style="list-style-type: none"> <li>- 9 voice mail</li> <li>- 2 urgent voice mail</li> <li>- 17 urgent e-mail</li> </ul> <p>The e-mail count does not include non-delivery receipts or meeting requests.</p>
Status	<p>Indicate whether to turn message notification to this device on or off. Subscribers can change this setting over the phone.</p> <ul style="list-style-type: none"> <li>• Enabled—Cisco Unity calls the device when there are new messages.</li> <li>• Disabled—Cisco Unity does not call the device. Disabling a device does not delete its settings.</li> </ul>
Notify Subscriber Of	<p>Select the types of messages and message urgency for which Cisco Unity will call the device. If no message type is selected, Cisco Unity does not call the device.</p> <p>When setting up a chain of message notification devices, select messages in this field only for the first device. If any message types are selected for any device other than the first, message notification for this device will commence immediately and will not wait for the notification failure of the previous device. Therefore, your notifications will not chain but all trigger at once.</p>
Notification Schedule	<p>In the grid, click the blocks to change between inactive (no notifications) and active (notifications okay). Note that you can set active and inactive hours for one day, then use Copy Day’s Schedule to copy the settings to other days.</p>
Copy Day’s Schedule	<p>To avoid clicking the same blocks for more than one day, use the Copy Day’s Schedule and &gt;&gt; functions. Select a day to copy, then select which days to copy the schedule setting to.</p>

Table 17-10 Subscribers &gt; Subscribers &gt; Message Notification Page (continued)

Field	Considerations
Notification Options: Send Initial Notification After How Many Minutes	<p>Specify the delay from the time a message is received until the message notification triggers (if the message matches the criteria selected in the Notify Subscriber Of section). You can space notifications on different devices at regular intervals, such as 15 minutes, to achieve a cascading message notification effect.</p> <p>If the delay time takes the notification out to a time when the device schedule is no longer active, the notification does not take place.</p> <p>The range for the delay field is 0 to 120 minutes. The default is 0 minutes.</p>
Notification Options: Restart Notification or Repeat Notification	<p>Use to specify the timing of message notification according to subscriber needs. Choose one of these options:</p> <ul style="list-style-type: none"> <li>Restart Notification Each Time a New Message Arrives—When this option is selected, Cisco Unity begins a notification process immediately upon the arrival of each message that matches the selected criteria. Cisco Unity considers notification successful if the device answers, even if new messages remain. (For example, notification is considered successful even when an answering machine picks up and records the message, but the message remains unread in the e-mail Inbox.)</li> </ul> <p>Note that if you activate the Restart Notification option and the Send Initial Notification field is set to 0, then Cisco Unity triggers the message notification immediately. However, if you enter a delay in the Send Initial Notification field, then Cisco Unity delays notification that number of minutes instead of dialing immediately. Messages that arrive during the delay period will not trigger separate notifications.</p> <ul style="list-style-type: none"> <li>Repeat Notification If There Are Still New Messages After This Many Minutes—When this option is selected and a duration specified, Cisco Unity attempts notification immediately after the first message, and then initiates a notification schedule based on the specified interval. For example, if you set the repeat notification interval to 5 minutes at 11:47 AM, Cisco Unity will notify the subscriber of new messages at 11:50 AM, 11:55 AM, 12:00 PM, 12:05 PM, 12:10 PM, 12:15 PM, 12:20 PM, 12:25 PM, and so on. The notification schedule is effective for as long as the subscriber has one or more new messages.</li> </ul> <p>The range for the redial frequency field is 1 to 100 minutes.</p>
If Device Does Not Answer <i>(not available for text pager notifications)</i>	<p>Indicate settings for the following:</p> <ul style="list-style-type: none"> <li>Wait for How Many Rings Before Hanging Up—Set to a minimum of 3 rings. Choose a higher number to give a subscriber more time to get to the phone.</li> <li>Try Again How Many Times—Choose a higher number to reach a subscriber who steps away from the phone briefly. Choose a lower number to avoid disturbing others.</li> <li>How Many Minutes to Wait Between Tries—Choose a higher number to reach a subscriber who is away from the phone for long periods of time.</li> </ul>
If Device Is Busy <i>(not available for text pager notifications)</i>	<p>Indicate settings for the following:</p> <ul style="list-style-type: none"> <li>Try Again How Many Times—Choose a higher number to reach a subscriber who uses the phone frequently.</li> <li>How Many Minutes to Wait Between Tries—Choose a higher number to reach a subscriber who has long phone conversations.</li> </ul>

**Table 17-10 Subscribers > Subscribers > Message Notification Page (continued)**

Field	Considerations
If Notification Fails, Send Notification To <i>(not available for text pager notifications)</i>	Select an option for an additional device to send notification to when the first device does not answer or is busy, and the maximum number of retries has been reached. Cisco Unity calls the next device only if it is enabled and its schedule is current.  Cisco Unity considers message notification successful if a device answers, even if, for example, an answering machine answers. Cisco Unity considers that message notification has failed only after all selected no-answer and busy signal retries have been exhausted.
Switch <i>(for dual phone system integrations only)</i>	Select the phone system that Cisco Unity dials out on when notifying the subscriber of new messages. Each notification device (except for text pagers) can be associated with a specific phone system.  On the System > Ports page, the selected phone system must have at least one port set to dial out for message notification.

## Subscriber Alternate Extension Settings

In addition to the “primary” extension that you assign subscribers, you can also assign subscribers up to nine alternate extensions. (The primary extension is the one that you assign to each subscriber when you create his or her subscriber account; it is listed on the Subscribers > Subscribers > Profile page.) If you have more than one Cisco Unity server that accesses a single, corporate-wide directory, you may want to add alternate extensions so that a subscriber uses the same number when addressing a message to a subscriber associated with another Cisco Unity server and when calling that subscriber directly.

Even if assigning alternate extensions is not necessary in your situation, you may want to add them as a convenience for subscribers. For example, alternate extensions can be used to:

- Handle multiple line appearances on subscriber phones.
- Offer easy message access on direct calls from a cell phone, home phone, or phone at an alternate work site (assuming that the phone number is passed along to Cisco Unity from these other phone systems). In addition, when such phones are used as alternate extensions, and are set to forward to Cisco Unity, callers can listen to the subscriber greeting, and leave messages for the subscriber just as they would when dialing the primary extension for the subscriber.
- Simplify addressing messages to subscribers at different locations. With alternate extensions, the number that a subscriber uses when addressing a message to someone at another location can be the same number that the subscriber dials when calling.
- Enable URL-based extensions in Cisco Unity for an integration with a SIP phone system.

Alternate extensions utilize the same transfer settings as the primary extension. In many cases, Cisco Unity can activate a message waiting indicator (MWI) for an alternate extension. Note that depending on the phones and phone systems involved, some additional phone system programming may be required to set this up.

## Setting Up Alternate Extensions

Do the applicable procedure to add, modify, or delete alternate extensions:

- [To Add Alternate Extensions, page 17-26](#)
- [To Modify or Delete Alternate Extension\(s\), page 17-27](#)

### To Add Alternate Extensions

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Alternate Extensions** page.
- Step 2** Click the **Add** button.
- Step 3** In the Alternate Extensions table, enter an extension up to 30 characters in length in the field provided. Each alternate extension that you add must be unique; Cisco Unity will not accept an extension that is already assigned to another subscriber (either as a primary or alternate extension), or to a public distribution list, call handler, directory handler, or interview handler. If your site has multiple Cisco Unity servers that are grouped together, this restriction applies to extensions used throughout the dialing domain.
- When entering characters in the Alternate Extensions table, consider the following:
- Enter digits 0 through 9.
  - Enter a valid URL (SIP integrations only).
  - Do not use spaces, dashes, or parentheses.
- Step 4** Click the **Save** icon. Alternate extensions are enabled for all rows in the table.
- Step 5** Repeat Step 2 through Step 4 as necessary.



#### Note

You can run the Cisco Unity Bulk Import wizard when you want to add alternate extensions for multiple subscribers at once.

Use the following table to learn more about subscriber alternate extension settings.

**Table 17-11 Subscribers > Subscribers > Alternate Extensions Page**

Field	Considerations
Alternate Extensions	<p>For each alternate extension that you want to assign, click Add, and then enter the extension in the field provided.</p> <p>You can assign subscribers up to nine alternate extensions. Each must be unique—up to the dialing domain level, if applicable—and no more than 30 characters in length.</p> <p>When entering characters in the Alternate Extensions table, consider the following:</p> <ul style="list-style-type: none"> <li>• Enter digits 0 through 9.</li> <li>• Do not use spaces, dashes, or parentheses between characters.</li> <li>• (SIP integrations only) Enter a valid URL.</li> </ul> <p>Use when setting up Digital Networking, when handling multiple line appearances on subscriber phones, when handling alphanumeric extensions, or as a convenience for subscribers and callers who want to communicate by using a cell phone, home phone, or phone at an alternate work site in addition to a subscriber phone.</p>
Select All	Click Select All and then click Delete to remove all alternate extensions from the table.
Clear All	Click Clear All to deselect the alternate extensions that you had selected to delete.
Delete	Check the box(es) next to the alternate extension(s) that you want to delete, or click Select All, and then click Delete to remove one or more alternate extensions from the table.

Table 17-11 Subscribers &gt; Subscribers &gt; Alternate Extensions Page (continued)

Field	Considerations
Add	<p>Enter the extension in the field provided for each alternate extension that you want to assign. Click the Save icon to update the subscriber record. Click Add to create another alternate extension.</p> <p>You can assign subscribers up to nine alternate extensions (for a total of 10 extensions). Each must be unique—up to the dialing domain, if applicable—and no more than 30 digits in length (SIP integrations can use up to 30 alphanumeric characters).</p> <p>To activate message waiting indicators (MWIs) for an alternate extension, enter the appropriate number into the MWI Extensions table on the Subscribers &gt; Subscribers &gt; Messages page.</p>

#### To Modify or Delete Alternate Extension(s)

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Alternate Extensions** page.
- Step 2** Do any of the following:
- To modify an extension, change the extension in the Alternate Extensions table as applicable.
  - To delete extensions, check the check boxes next to the alternate extensions that you want to delete, and then click **Delete**.
  - To remove all alternate extensions listed in the table, click **Select All**, and then click **Delete**.
- Step 3** Click the **Save** icon.
- Step 4** Repeat [Step 2](#) through [Step 3](#) as necessary.
-





# Public Distribution List Settings

## Overview: Public Distribution Lists

Public distribution lists are used to send voice messages to multiple subscribers. The subscribers assigned to a public distribution list typically are subscribers who need the same information on a regular basis, such as employees in a department or members of a team. The class of service that is associated with each subscriber account dictates whether subscribers can send messages to public distribution lists in Cisco Unity.

## Predefined Public Distribution Lists

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

<b>All Subscribers</b>	By default, the All Subscribers list is included in the {Default Subscriber} template. When subscribers are created, they are automatically added to this list.
<b>Unaddressed Messages</b>	Subscribers assigned to the Unaddressed Messages list receive messages left in the Operator call handler when the operator is not available. Additionally, when the Cisco Unity Messaging System receives a nondelivery receipt (NDR) for a voice message, it is forwarded to the Unaddressed Messages list.  When Cisco Unity is installed, the Example Administrator account is set as the only member of the Unaddressed Messages and System Event Messages distribution lists. Do not delete the Example Administrator account unless you have assigned the applicable subscriber(s) or another distribution list to review the messages sent to these two distribution lists. In addition, note that if you later delete the assigned subscribers or distribution lists, Cisco Unity does not prompt you to assign a replacement.
<b>System Event Messages</b>	The System Event Messages distribution list can be used to send event notification messages from the Event Monitoring Service (EMS). Note that by default, the System Event Messages distribution list is set up to contain the Example Administrator as its only member. To send these messages to system administrators, remove Example Administrator and add the applicable subscribers to the list.

In each subscriber template, you can specify the public distribution lists to which each new subscriber based on that template will be added. You can also add individual subscribers directly to the public distribution lists. When you delete a subscriber account, Cisco Unity automatically removes the subscriber from any public distribution list of which the subscriber is a member.

See the following sections in this chapter for more information:

- [Creating and Modifying Public Distribution Lists, page 18-2](#)
- [Public Distribution List Profile Settings, page 18-3](#)
- [Public Distribution Lists Members Settings, page 18-3](#)

## Creating and Modifying Public Distribution Lists

You can modify the predefined lists, and you can create new ones. Additionally, you can import public distribution lists from Domino. Both Cisco Unity subscribers and non-subscribers are included as members of an imported distribution list, though non-subscribers are not displayed in the Cisco Unity Administrator.

Messages addressed to an imported list are sent to all members of the list, including those who are not Cisco Unity subscribers.

Use the following procedures to create or modify a public distribution list.

### To Create a Public Distribution List

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Public Distribution List dialog box, enter information as applicable in the Name field.
- Step 4** Do one of the following:
- Select **New Distribution List**.
  - Select **Based on Existing Distribution List**, and then select the applicable distribution list in the Based On field.
  - Select **Import**, and then click **Select**. In the Find and Select Public Distribution List to Import dialog box, click the applicable address book from the list, and click **Find**. Double-click the applicable person document.
- Step 5** Click the **Add** button.
- Step 6** Enter settings for your new distribution list, and then click the **Save** icon.
- 

### To Modify a Public Distribution List

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.
- Step 2** Click the **Find** icon.
- On the Find and View Distribution List dialog box, in the Find By field, select Name or Dial ID search criteria, then enter the name or Dial ID of a distribution list to modify. You also can enter \* for a list of all distribution lists, or enter one or more characters of the name or Dial ID followed by \* to narrow your

search. Note that only one asterisk can be used when doing a wild card search, and the asterisk must be the last character in the search string. For example, the search string `co*` is allowed; the search strings `*co` and `*co*` are not allowed.

- Step 3** Click **Find**.
- Step 4** Double-click the distribution list that you want to modify.
- Step 5** Change settings as applicable, and then click the **Save** icon.

## Public Distribution List Profile Settings

The profile settings specify the name of the distribution list, its recorded voice name, and extension. A public distribution list must have either a recorded voice name or an assigned extension for subscribers to address messages to it.

Use the following table to learn more about profile settings.

**Table 18-1** *Subscribers > Public Distribution Lists > Profile Page*

Field	Considerations
Name	This displays the name of the public distribution list. To change the name of the list, enter a new name here, and then click the Save icon.
Owner	This setting displays the owner of the list, which can be any subscriber or another public distribution list that has the authority to request changes to this list.  To change the owner, select an Owner Type and click Change.
Owner Type	Click Subscriber to assign ownership to a single subscriber. Click Distribution List to assign ownership to all subscribers on a public distribution list.  Default: Subscriber.
Recorded Voice	This is the recorded name of the public distribution list.  To record a distribution list name, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.
Extension	Enter the number that subscribers can dial to access the public distribution list over the phone (without having to spell the list name). If an extension is provided, the list owner can administer the list over the phone.  Default: Blank.

## Public Distribution Lists Members Settings

The public distribution lists member settings allow you to:

- View the names of all members assigned to the list. As applicable, both Cisco Unity subscriber and non-subscriber members are displayed.
- Add subscribers and/or other public distribution lists to the list.
- Remove subscribers and/or other public distribution lists from the list.

### To Add or Remove Subscribers from a Public Distribution List

- 
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the name of the list that you want to modify.
- Step 4** Go to the **Subscribers > Public Distribution Lists > Members** page.
- Step 5** Click **Add** or **Remove**, as applicable. If you click **Add**, select either **Selected Subscribers** or **Public Distribution Lists** from the list on the right.
- Enter the name of a subscriber or distribution list to add or remove. You also can enter \* for a list of all subscribers or lists, or enter one or more characters followed by \* to narrow your search. Note that only one asterisk can be used when doing a wild card search, and the asterisk must be the last character in the search string. For example, the search string co\* is allowed; the search strings \*co and \*co\* are not allowed.
- Step 6** Click **Find**.
- Step 7** Select the subscriber or distribution list name to add or remove. To select more than one name, hold down the Ctrl or Shift key.
- Step 8** Click **Add to List** or **Remove**, as applicable.
- 

Use the following table to learn more about member settings.

**Table 18-2** *Subscribers > Public Distribution Lists > Members Page*

Field	Considerations
View, Add, Remove	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>View—Display a list of distribution list members.</li> <li>Add—Add one or more subscribers to the public distribution list. You also can add other public distribution lists as members of the list.</li> <li>Remove—Delete one or more subscribers or public distribution lists from the public distribution list.</li> </ul> <p>Default: View.</p>
Type a <Public Distribution List> Name to Find	<p>Enter several characters of the name, and click Find. Enter * to list all members or distribution lists, or enter one or more characters of the name or Dial ID followed by * to narrow your search.</p> <p>Note that only one asterisk can be used when doing a wild card search, and the asterisk must be the last character in the search string. For example, the search string co* is allowed; the search strings *co and *co* are not allowed.</p> <p>When Add is selected, Cisco Unity searches all subscribers in the organization. When Remove is selected, Cisco Unity searches only subscribers assigned to the distribution list.</p>
Matching <Public Distribution List> Members	<p>This setting displays the list of names that match the characters you entered in the Type a &lt;Public Distribution List&gt; Name to Find field. The list contains first and last names that match.</p> <p>To select several nonsequential names at one time, hold down the Ctrl key while selecting.</p> <p>To select several names in sequence, hold down the Shift key, select the first name in the sequence, and then select the last name in the sequence.</p>







## Account Policy Settings

---

### Overview: Account Settings

The account policy settings on the Phone Password Restrictions Page and the Cisco Unity Account Lockout Page in the Cisco Unity Administrator apply when subscribers access Cisco Unity by phone. Changes to settings in the account policy affect all existing subscribers.

Note that the settings on the Account Policy pages represent a different account policy from the one that applies when subscribers use web applications to access Cisco Unity. For information on specifying an account policy for the Cisco Personal Communications Assistant (PCA) and the Cisco Unity Administrator, see the [“Authentication Settings” section on page 28-11](#).

See the following sections in this chapter for more information:

- [Phone Password Restriction Settings, page 19-1](#)
- [Account Lockout Settings, page 19-3](#)

### Phone Password Restriction Settings

Phone password restriction settings allow you to define a system-wide password policy that applies when subscribers access Cisco Unity by phone. For greater security, establish rules that prevent passwords from being easy to guess and from being used for a long time. At the same time, it is also best to avoid requiring passwords that are so complicated or that must be changed so often that subscribers have to write them down to remember them. Consider requiring that subscribers use a long—eight or more digits—and non-trivial password when you specify phone password restrictions.

Phone password restrictions cannot be changed for individual subscriber accounts. However, you can use the password settings on the template and individual subscriber pages in the Cisco Unity Administrator to govern the passwords that subscribers initially use to log on to Cisco Unity by phone, and to define whether and when subscribers can change their own phone passwords. You can also use the Cisco Unity Bulk Import wizard to set phone passwords for multiple subscriber accounts at the same time. (Refer to the Cisco Unity Bulk Import online Help for details.)

Use the following table to learn more about phone password settings.

**Table 19-1** *Subscribers > Account Policy > Phone Password Restrictions Page*

Field	Considerations
Maximum Phone Password Age	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Password Never Expires—Subscribers are never prompted to change their passwords, although they are able to change passwords anytime.</li> <li>• Days Until Password Expires—Subscribers are prompted to change their passwords every X days. X is the value specified in the adjacent box.</li> </ul>
Phone Password Length	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Permit Blank Password—Subscribers are able to log on without entering a password. Note that this leaves subscriber messages vulnerable to unauthorized access.</li> <li>• Minimum Number of Characters—Subscribers are required to create a password at least X characters long. X is the value specified in the adjacent box. In general, shorter passwords are easier to use, but longer passwords are more secure. Eight or more digits is recommended.</li> </ul> <p>When you change the minimum password length, subscribers will be required to use the new length the next time they change their passwords.</p>
Phone Password Uniqueness	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Do Not Keep Password History—Cisco Unity does not compare a new password with previous passwords; thus a subscriber can reuse passwords.</li> <li>• Number of Passwords to Remember—Cisco Unity stores the specified number of previous passwords for a subscriber and compares a new password with them. Cisco Unity rejects the new password if it matches a password in the history.</li> </ul> <p>If the Permit Blank Password box is selected, the Phone Password Uniqueness fields are disabled.</p>
Check Against Trivial Passwords for Extra Security	<p>Check this check box to have Cisco Unity verify that a new password meets the following criteria:</p> <ul style="list-style-type: none"> <li>• The password is not the same as previous passwords.</li> <li>• The digits are not all the same (for example, 9999).</li> <li>• The digits are not consecutive (for example, 1234).</li> <li>• The password is not the same as the extension assigned to the subscriber.</li> <li>• The password does not spell the name of the subscriber.</li> </ul> <p>If the Permit Blank Password box is selected, the Check Against Trivial Passwords for Extra Security field is disabled.</p>

# Account Lockout Settings

Cisco Unity account lockout settings allow you to specify whether you want Cisco Unity to use an account lockout policy that applies to all subscribers who access Cisco Unity by phone. To customize the account lockout policy for your organization, you can use the settings on the Cisco Unity Account Lockout page to dictate:

- How Cisco Unity handles situations when subscribers attempt to log on to Cisco Unity by phone and repeatedly enter incorrect phone passwords.
- The number of failed logon attempts that are allowed before Cisco Unity prohibits the subscriber from accessing Cisco Unity by phone.
- The length of time that a subscriber who is locked out must wait before attempting to access Cisco Unity by phone again.

Changes to account policy settings affect all Cisco Unity subscribers. You cannot change account policy settings for individual subscriber accounts, though you can lock individual subscriber accounts to prevent subscribers from using the phone to access Cisco Unity. (For details, see the [“Subscriber Account Settings”](#) section on page 17-4.)

Use the following table to learn more about account lockout settings.

**Table 19-2** *Subscribers > Account Policy > Unity Account Lockout Page*

Field	Considerations
No Account Lockout	Click this option if you do not want to specify an account lockout policy for subscribers using the phone to access Cisco Unity. When this option is selected, Cisco Unity allows unlimited logon attempts to a subscriber account.
Account Lockout	Click this option if you want to specify an account lockout policy for subscribers using the phone to access Cisco Unity. When this option is selected, enter the applicable values in the following fields: <ul style="list-style-type: none"> <li>• Lock Account After __ Invalid Attempts</li> <li>• Reset Count After __ Minutes</li> <li>• Lockout Duration</li> </ul>
Lock Account After __ Invalid Attempts	Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by phone.  This option is unavailable when the No Account Lockout option is selected.
Reset Count After __ Minutes	Enter the number of minutes after which Cisco Unity will clear the count of failed logon attempts to Cisco Unity by phone (unless the failed logon limit is already reached and the account is locked).  This option is unavailable when the No Account Lockout option is selected.

Table 19-2 Subscribers &gt; Account Policy &gt; Unity Account Lockout Page (continued)

Field	Considerations
Lockout Duration	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Forever—When you select this option, Cisco Unity will prevent subscribers from accessing Cisco Unity by phone until a system administrator unlocks the subscriber account on the Subscribers &gt; Subscribers &gt; Account Page for an individual subscriber. Use this setting only if a system administrator is readily available to assist subscribers or if the system is prone to unauthorized access.</li> <li>• Minutes—When you select this option, enter the number of minutes that Cisco Unity will prevent subscribers from accessing Cisco Unity by phone. Cisco Unity allows subscribers to access Cisco Unity by phone after the specified number of minutes has elapsed. Use this setting if a system administrator may not be available to assist subscribers; avoid using if the system is prone to unauthorized access.</li> </ul> <p>This option is unavailable when the No Account Lockout option is selected.</p>



# Call Management

---

## Overview: Cisco Unity Call Management

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

### Call Handlers

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 subscribers and to other call handlers; and play audiotext (prerecorded information). See the [“Overview: Call Handler Settings” section on page 21-1](#) for more information.

### Directory Handler

Directory handlers provide directory assistance by playing an audio list that subscribers and unidentified callers use to reach subscribers and to leave messages. See the [“Overview: Directory Handler Settings” section on page 22-1](#) for more information.

### Interview Handlers

Interview handlers collect information from callers by playing a series of questions and then recording the answers. See the [“Overview: Interview Handler Settings” section on page 23-1](#) for more information.

### Call Routing Tables

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. Once you have set up call handlers, interview handlers, and the directory handler, as well as extensions for subscribers, you can route calls to the applicable person or handler by modifying the call routing tables. See the [“Overview: Call Routing Tables” section on page 24-1](#) for more information.

### Restriction Tables

Restriction tables control outgoing calls by allowing you to specify the numbers that Cisco Unity can dial for transferring calls, for notifying subscribers of messages, and for delivering faxes. See the [“Overview: Restriction Tables” section on page 25-1](#) for information on how to set up and use restriction tables.

## 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.

### Routing Callers by Using One-Key Dialing

With one-key dialing, you can offer callers a menu of choices. One-key dialing enables you to designate a single digit to represent a subscriber extension, call handler, interview handler, or directory handler. Instead of entering the full extension, the caller presses a single key.

Callers can 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 way you have set up a one-key dialing menu. These pauses allow callers to press full extension IDs to bypass one-key dialing menus, even during the handler greeting.

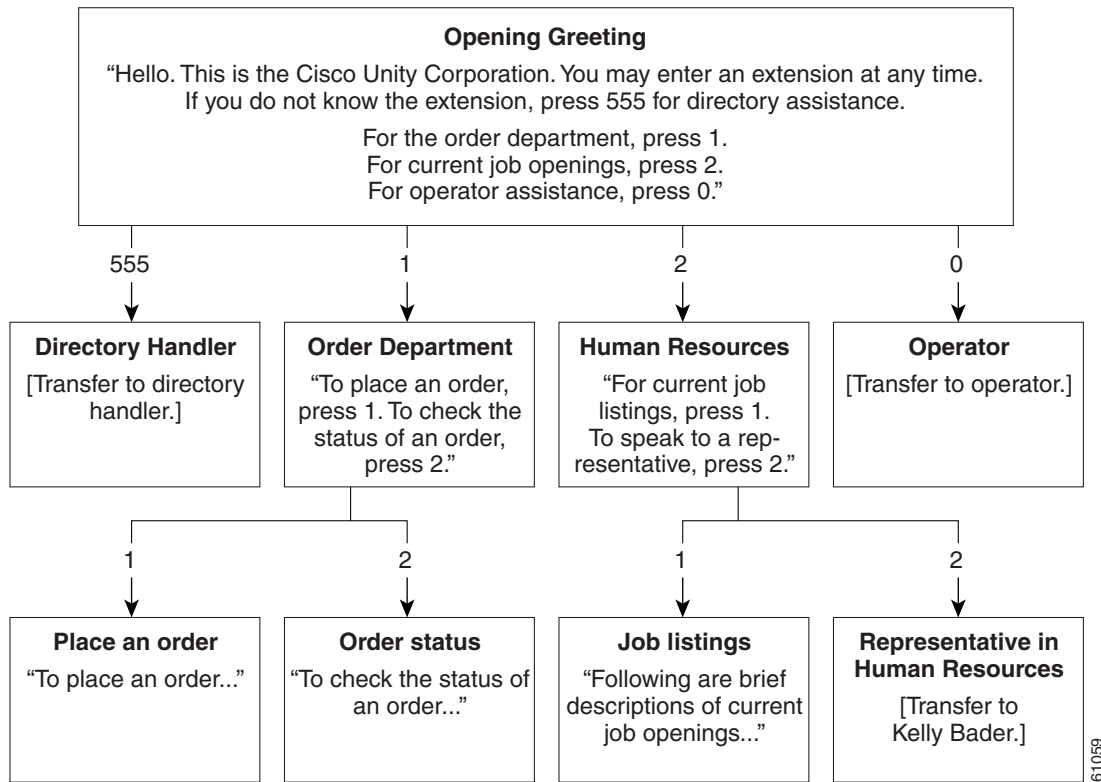
You can also lock certain keys to take the caller directly to the action programmed for that key without waiting for an additional key press.

Use the handler greeting to tell callers about the one-key options they have, and whether they are allowed to enter an extension during the greeting.

### Creating a Call Management Map

Once 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 call handlers in your plan. See [Figure 20-1](#) for a sample call management map that makes use of the automated attendant.

Figure 20-1 Sample Automated Attendant Call Management Map



61059

## 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 will select these “destination” call handlers when you create the call handlers that route calls to them. You also need to create Cisco Unity accounts for the subscribers to which call handlers will transfer before creating those call handlers.

Using [Figure 20-1](#) as an example, you first create a subscriber 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 20-1](#), 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. See the [“Overview: Call Routing Tables”](#) section on [page 24-1](#) for more information.





## Call Handler Settings

---

### Overview: Call Handler Settings

Call handlers answer calls, greet callers with recorded prompts and provide them with information and options, route calls, and take messages. They are a basic component of Cisco Unity. Your plan for call handlers can be simple, using only the predefined Cisco Unity call handlers, or you can create an unlimited number of 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 touchtones. 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.”).
- 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 subscriber (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.

See the [“Creating a Call Management Plan”](#) section on page 20-2 for information about using call handlers and other call management tools to manage incoming calls.

## Predefined Call Handlers

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

<b>Opening Greeting</b>	<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 Default Call Handler 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 dial the applicable extension to reach the Sign-in conversation, or the Operator call handler. Messages left in the Opening Greeting call handler are sent to the Example Administrator. See the Call Management &gt; Call Handlers &gt; Opening Greeting pages for details on additional settings.</p>
<b>Operator</b>	<p>Calls are routed to this call handler when callers press “0” or do not press any key, (the default setting) as stated in the Cisco Unity conversation. You can set up 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 Unaddressed Messages distribution list. See the Call Management &gt; Call Handlers &gt; Operator pages for details on additional settings.</p>
<b>Goodbye</b>	<p>Plays a brief goodbye message and then hangs up if there is no caller input. By default, the Goodbye call handler allows callers to dial the applicable extension to reach the Sign-in conversation, or the Operator call handler. If you change the After Greeting action from Hang Up to Take Message, then messages left in the Goodbye call handler are sent to the Example Administrator. See the Call Management &gt; Call Handlers &gt; Good-bye pages for details on additional settings.</p>

See the following sections in this chapter for more information:

- [Creating and Modifying Call Handlers, page 21-2](#)
- [Call Handler Profile Settings, page 21-5](#)
- [Call Handler Transfer Settings, page 21-7](#)
- [Call Handler Greetings Settings, page 21-10](#)
- [Call Handler Caller Input Settings, page 21-12](#)
- [Call Handler Messages Settings, page 21-13](#)

## Creating and Modifying Call Handlers

You can use the following procedures in this section to create new call handlers, or modify existing ones from the Call Management > Call Handler pages of the Cisco Unity Administrator. You can also use the Bulk Edit utility to make changes to multiple call handlers at once. The Bulk Edit utility is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop.)

To manage call handler greetings when you—or the call handler owner(s) that you assign—cannot access the Cisco Unity Administrator, you can use the Cisco Unity Greetings Administrator. For more information, see the [“Setting Up the Cisco Unity Greetings Administrator”](#) section on page 21-3 and the [“Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings”](#) section on page 21-5.

---

#### To Create a New Call Handler in the Cisco Unity Administrator

- 
- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Call Handlers** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Call Handler dialog box, enter information as applicable in the Name field.
- Step 4** Select **New Handler** or **Based on Existing Handler**. If you select Based on Existing Handler, select the applicable call handler in the Based On field.
- Note that if you based your new call handler on an existing one, you reuse all of the settings, including recorded greetings. For this reason, make sure to rerecord the greeting for the new call handler.
- Step 5** Click the **Add** button.
- Step 6** Enter settings for your new call handler, and then click the **Save** icon.
- 

---

#### To Modify a Call Handler in the Cisco Unity Administrator

- 
- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Call Handlers** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the call handler that you want to modify.
- Step 4** Change settings as applicable, and then click the **Save** icon.
- 

## Setting Up the Cisco Unity Greetings Administrator

The Cisco Unity Greetings Administrator allows you—or the call handler owner(s) that you assign—to manage call handler greetings from any phone. For example, when the office is unexpectedly closed because of bad weather, you can call Cisco Unity from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.

The owner of the call handler can be any subscriber or public distribution list. When a public distribution list owns a call handler, the Cisco Unity Greetings Administrator allows each member of the public distribution list to manage call handler greetings by using the Cisco Unity phone conversation. (Note that a call handler owner is not necessarily the message recipient.)

By using the Cisco Unity Greeting Administrator, you can do the following tasks without having to access the Cisco Unity Administrator:

- Rerecord a call handler greeting.
- Enable or disable the alternate greeting for a call handler.
- Determine which greeting is currently active for a call handler.

### Task List for Setting Up the Cisco Unity Greetings Administrator

1. Set up a phone number so that you or another subscriber can call the Cisco Unity Greetings Administrator. To do so, refer to the documentation for the phone system.
2. Add a routing rule to forward calls from the phone number that you set up to the Cisco Unity Greetings Administrator. Do the procedure [“To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator.”](#)
3. Assign a unique extension to the call handler. Do the procedure [“To Assign a Unique Extension to the Call Handler.”](#) Repeat for each call handler that you want to access by using the Cisco Unity Greetings Administrator.
4. As needed, tell call handler owners how to use the Cisco Unity Greetings Administrator. See the [“Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings”](#) section on page 21-5.



#### Note

The RSA SecurID system is not available for subscribers who use the Cisco Unity Greetings Administrator. (For information on RSA SecurID, see the [“Enhanced Phone Security”](#) chapter.)

### To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator

- Step 1** Go to the **Call Management > Call Routing > Direct Calls** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Call Routing Rule – Direct dialog box, enter a name for the new routing rule, and click **Add**.
- Step 4** In the Status field, confirm that Enabled is selected.
- Step 5** In the Dialed Number field, enter the phone number that is set up for the system administrator to dial for changing call handler greetings by phone.
- Step 6** In the Send Call To field, click **Greetings Administrator**.
- Step 7** Change other fields for the routing rule as needed.
- Step 8** In the routing table at the bottom of the page, confirm that the new routing rule is in an appropriate position with the other routing rules.  
To change the order of the routing rules, click **Change Rule Order**. (For information on routing rule order, see the [“How Call Routing Rules Work”](#) section on page 24-2.)
- Step 9** Click the **Save** icon.

### To Assign a Unique Extension to the Call Handler

- Step 1** In the Cisco Unity Administrator, go to the **Call Management > Call Handlers > Profile** page.
- Step 2** Click the **Find** icon, and in the Select and View dialog box, click **Find**. A list of call handlers appears.
- Step 3** Click the call handler that you want to access by using the Cisco Unity Greetings Administrator and click **View**.
- Step 4** In the Extension field, enter the unique extension you want to assign to the call handler.
- Step 5** Click the **Save** icon.

## Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings

Once you have set up the Cisco Unity Greeting Administrator for a call handler, the owner of the call handler can toggle between the alternate and standard call handler greetings, or record the call handler greeting over the phone. When a public distribution list owns a call handler, the Cisco Unity Greetings Administrator allows each member of the public distribution list to manage call handler greetings by using the Cisco Unity phone conversation.

To access the Cisco Unity Greetings Administrator, the owner of the call handler will require the following information:

- The phone number to dial for access to the Cisco Unity Greetings Administrator
- 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 Cisco Unity, 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.
- Step 5** Follow the Cisco Unity conversation to toggle between the alternate and standard call handler greetings, or to record the call handler greeting.

<b>Toggle between greetings</b>	Press <b>1</b> .
<b>Record the greeting</b>	Press <b>2</b> .

---

## Call Handler Profile Settings

The profile settings specify who owns the call handler, which schedule controls transfer settings and greetings, and the extension of the call handler.

Use the following table to learn more about profile settings.

**Table 21-1** Call Management > Call Handlers > Profile Page

Field	Considerations
Name	This displays the name of the call handler. To change the name of the call handler, enter a new name here, and then click the Save icon.

Table 21-1 Call Management &gt; Call Handlers &gt; Profile Page (continued)

Field	Considerations
Created	<i>Display only.</i> This setting shows the date and time that the call handler was created.
Owner	To change the owner, select an Owner Type and click Change.  The owner can be any subscriber or public distribution list. The owner of the call handler can record and change the call handler greeting over the phone. Note that the owner is not necessarily the message recipient.
Owner Type	Click Subscriber to assign ownership to a single subscriber. Click Public Distribution List to assign ownership to all subscribers on a public distribution list.  Default: Subscriber.
Recorded Voice	This is the recorded name of the call handler.  To record a call handler name, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.
Active Schedule	Select the schedule to determine the times that standard and closed transfer rules and greetings are in effect for the call handler. To view details of the selected schedule, click the View link. Note that when you click the link, you leave this page and move to the System > Schedules page.  Default: Weekdays.
Extension	Enter the extension, if any, that callers dial to reach the call handler. Assign an extension only if you plan to allow callers to dial the number.  When the call handler is reached only from one-key caller input, do not enter an extension here.  Note that this extension is not the same as the extension to which calls are transferred. The extension to which calls are transferred is set on the Call Management > Call Handlers > Call Transfer page.  Default: Blank.
Language	Select the language in which Cisco Unity plays the handler system prompts. If you choose Inherited, Cisco Unity determines the language to use for system prompts on a per-call basis, depending on the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.  The default phone language and the list of languages shown here are set on the System > Configuration > Phone Languages page.  Default: Inherited.
Switch <i>(for dual phone system integrations only)</i>	Select the phone system that the call handler uses. If this setting is incorrect, Cisco Unity will not be able to transfer calls to or from the call handler.

# Call Handler Transfer Settings

Call transfer settings specify whether unidentified callers are transferred to a phone or to the greetings of a subscriber or handler. These settings also specify how Cisco Unity handles a transfer: Cisco Unity can either release the call to the phone system, or it can supervise the transfer.

When Cisco Unity is set to supervise transfers, it can provide additional call control with call holding and call screening:

- With call holding, when the phone is busy, Cisco Unity can ask callers to hold. Cisco Unity plays hold music, and approximately every 30 seconds, tells callers on hold how many callers are ahead of them and allows them to continue holding, leave a message, or try another extension. There is no limit to the number of callers that can be holding.

If call holding is not selected, callers are sent to whichever subscriber or handler greeting is enabled—either the busy, standard, closed, or alternate greeting.

- With call screening, Cisco Unity can ask for the name of the caller before connecting to a subscriber. The subscriber can then hear who is calling and, when a phone is shared by more than one subscriber, who the call is for. The subscriber can then accept or refuse the call.

Each call handler can have three transfer rules which you can customize: one for standard hours and one for closed 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.

Use the following table to learn more about transfer settings.

**Table 21-2** Call Management > Call Handlers > Call Transfer Page

Field	Considerations
Transfer Rule Applies To	<p>The settings on the rest of the page apply to the transfer rule selected here: either standard, closed, or alternate.</p> <p>The schedule that is used to determine the times that standard and closed transfer rules and greetings are in effect is set on the Profile page for the call handler. When enabled, the alternate transfer rule overrides the standard and closed transfer rules and is in effect at all times.</p>
Status	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Enabled—The transfer rule is active and Cisco Unity directs callers as defined by the settings within this rule.</li> <li>• Disabled—The transfer rule is inactive and Cisco Unity ignores all settings within this rule.</li> </ul> <p>When Transfer Rule Applies To is set to Standard, this setting is automatically set to Enabled, and it cannot be changed.</p> <p>Default: Enabled.</p>

Table 21-2 Call Management &gt; Call Handlers &gt; Call Transfer Page (continued)

Field	Considerations
Transfer Incoming Calls	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• No (Send Directly)—Cisco Unity transfers the call to the call handler greeting.</li> <li>• Yes, Ring the Recipient—Cisco Unity transfers calls to the extension assigned to the message recipient. Cisco Unity displays the name and extension in the adjacent box. The message recipient is set on the Messages page of the call handler.</li> <li>• Yes, Ring Subscriber—Cisco Unity transfers calls to the number entered in the adjacent box. The number can be an extension or any phone number. Use digits 0 through 9, *, and #. You can also enter , (comma) to insert a one-second pause.</li> </ul> <p>Default: No (Send Directly).</p>
Transfer Type	<p>Select how Cisco Unity transfers calls. Use this setting with caution and only if you understand its implications on the phone and voice messaging systems.</p> <ul style="list-style-type: none"> <li>• Release to Switch—Cisco Unity puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or not answered, the phone system forwards the call to Cisco Unity, then Cisco Unity routes the call to the subscriber or handler greeting. This transfer type allows Cisco Unity to process incoming calls more quickly. Use Release to Switch only when call forwarding is enabled on the phone system.</li> <li>• Supervise Transfer—Cisco Unity acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Cisco Unity—not the phone system—forwards the call to the subscriber or handler greeting. You can use supervised transfer whether or not the phone system forwards calls.</li> </ul> <p>The Transfer Type option is unavailable when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: Release to Switch.</p>
Rings to Wait For	<p>Select the number of times the extension rings before Cisco Unity plays the subscriber or handler greeting.</p> <p>Set this value to at least 2 to give subscribers a chance to answer. Avoid setting to more than 4, especially if the call may be transferred to another extension, where the caller might have to wait for another four rings. This value should be at least two rings fewer than the phone system setting for forwarding calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: Two rings.</p>

Table 21-2 Call Management &gt; Call Handlers &gt; Call Transfer Page (continued)

Field	Considerations
If the Call Is Busy	<p>Select the action that Cisco Unity performs for unidentified callers when the subscriber phone is busy. You may want to use holding options sparingly, because having calls on hold can tie up ports.</p> <ul style="list-style-type: none"> <li>• Always Hold—Cisco Unity plays a prompt indicating that the extension is busy. The caller is put on hold. Note that this hold is not performed by the phone system.</li> <li>• No Holding—Cisco Unity prompts the caller to leave a message and allows the caller to dial another extension.</li> <li>• Ask Caller—Cisco Unity gives the caller the options of holding, leaving a message, or dialing another extension.</li> </ul> <p>These options are unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: No Holding.</p>
Announce	<p>Check this check box to have Cisco Unity say “transferring call” when the subscriber answers the phone, to indicate that the call is from an unidentified caller.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: Check box not checked.</p>
Introduce (Call for Name)	<p>Check this check box to have Cisco Unity say “call for &lt;recorded name of the call handler&gt;” when the message recipient answers the phone. This setting applies only to calls from unidentified callers. Use this setting if the subscriber who is the message recipient takes calls for more than one dialed extension. The introduction alerts the subscriber who answers that the call is for the call handler.</p> <p>This option is unavailable when Release to Switch is checked and when Transfer Incoming Calls is set to No (Send Directly).</p> <p>Default: Check box not checked.</p>
Confirm (Call Can Be Accepted or Refused)	<p>Check this check box to have Cisco Unity prompt the subscriber to accept or refuse a call from an unidentified caller. If the call is accepted, it is transferred to the subscriber phone. If the call is refused, Cisco Unity plays the applicable subscriber greeting. You use this setting with the Ask Caller’s Name setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: Check box not checked.</p>
Ask Caller’s Name	<p>Check this check box to have Cisco Unity prompt unidentified callers to say their names. When the phone is answered, the subscriber hears “Call from...” before Cisco Unity transfers the call. You use this setting with the Confirm setting to allow the subscriber to screen calls.</p> <p>This option is unavailable when Release to Switch is selected and when Transfer Incoming Calls is set to the No (Send Directly) option.</p> <p>Default: Check box not checked.</p>

# Call Handler Greetings Settings

Each subscriber and call handler can have up to five greetings. The greeting settings specify which greetings are enabled and the actions that Cisco Unity takes during and after each greeting. Enabling a greeting makes it available for Cisco Unity to use in applicable situations.

The greeting that plays when a caller reaches a subscriber or call handler depends on:

- The active schedule.
- The greeting source.
- Whether the call is internal.
- Whether the called extension is busy.

Cisco Unity greetings for subscribers and call handlers are:

<b>Standard</b>	Plays at all times unless overridden by another greeting.
<b>Closed</b>	Plays during the closed (nonbusiness) hours defined for the active schedule. When in effect (when enabled and during closed hours), the closed greeting overrides the standard greeting, and thus limits the standard greeting to the open hours defined for the active schedule.
<b>Internal</b>	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 and closed greetings for internal calls. Not all phone system integrations provide the support necessary for an internal greeting. Note that the internal greeting must be enabled and recorded from the Cisco Unity Administrator or the Cisco Unity Assistant <sup>*</sup> ; subscribers cannot modify it by using the Cisco Unity subscriber conversation.
<b>Busy</b>	Plays when the extension is busy. (For example, “All of our operators are with other customers.”) A busy greeting overrides the standard, closed, and internal greetings. Not all phone system integrations provide the support necessary for a busy greeting. Note that the busy greeting must be enabled and recorded from the Cisco Unity Administrator or the Cisco Unity Assistant <sup>*</sup> ; subscribers cannot modify it by using the Cisco Unity subscriber conversation.
<b>Alternate</b>	Can be used for a variety of special situations, such as vacations or a holiday. (For example, “I will be out of the office until....”) An alternate greeting overrides all other greetings.

<sup>\*</sup>Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.

Call handler owners can select a different call handler greeting or record the call handler greetings from the Call Management > Call Handlers > Greetings page in the Cisco Unity Administrator, or they can use the Cisco Unity Greetings Administrator to do so over the phone. For more information, see the [“Setting Up the Cisco Unity Greetings Administrator”](#) section on page 21-3 and the [“Using the Cisco Unity Greetings Administrator to Change Call Handler Greetings”](#) section on page 21-5.

Use the following table to learn more about greeting settings.

**Table 21-3 Call Management > Call Handlers > Greetings Page**

Field	Considerations
Greeting	Select the greeting that you want to specify settings for. This setting does not reflect which of the greetings is active.
Status	Indicate whether the selected greeting is enabled. When a greeting is enabled, Cisco Unity plays it in the applicable situation. Recording a greeting does not automatically enable it; it must be enabled here.
Source	<p>Indicate the source for the greeting selected in the Greeting field:</p> <ul style="list-style-type: none"> <li>• System—Select to use the prerecorded system default greeting.</li> <li>• Recording—Select to use a personal recording for the subscriber (or call handler). To record and play greetings here, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.</li> <li>• Blank—Select to have no recording. When the greeting source is left blank, Cisco Unity immediately performs the after-greeting action.</li> </ul> <p>Default: Recording.</p>
Allow Caller Input	<p>Check this check box to enable settings specified on the Caller Input page. These settings contain actions assigned to caller key presses during the greeting. (For example, “To speak to my assistant, press 3.”)</p> <p>Click the Caller Input link to view the Caller Input page. Note that when you click the link, you leave the Greetings page.</p> <p>Default: Check box checked.</p>
After Greeting	<p>Indicate the action that Cisco Unity performs after the greeting plays:</p> <ul style="list-style-type: none"> <li>• Take Message—Cisco Unity records a message from the caller. Click the Take Message link to view the Messages page.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul> <p>Default: Send Caller to Hang Up.</p>

**Table 21-3** Call Management > Call Handlers > Greetings Page (continued)

Field	Considerations
Reprompt the User After this Many Seconds of Silence	Check this check box and enter a value in the field on the right to indicate the number of seconds of silence to allow. When Cisco Unity receives no input from a caller within this number of seconds, Cisco Unity prompts the caller again.  Default: Two seconds.
Number of Times to Reprompt	Indicate the number of times to reprompt a caller. After the number of times indicated here, Cisco Unity performs the after-greeting action.  Default: One time.

## Call Handler Caller Input Settings

Caller input settings define actions that Cisco Unity takes in response to touchtone keys pressed by callers. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page.

When recording the greeting for the call handler, remember to mention the choices for caller input in the call handler greeting. (For example, “For Sales, press 1; for Service, press 2; to speak to an operator, press 0.”)

Use the following table to learn more about caller input settings.

**Table 21-4** Call Management > Call Handlers > Caller Input Page

Field	Considerations
Allow Callers to Dial an Extension During Greeting	Check this check box to allow callers to enter an extension while the greeting plays. Use in conjunction with the Lock This Key check box to allow callers to enter some extensions but not others.  This option is unavailable if the Allow Caller Input check box is unchecked on the Greetings page.  Default: Check box checked.
Milliseconds to Wait for Additional Digits	Indicate the amount of time Cisco Unity waits for additional input after callers press a single key that is not locked. If there is no input within this time, Cisco Unity performs the action assigned to the single key.  A value of 1,500 (one and one-half seconds) is recommended.  This option is unavailable if the Allow Callers to Dial check box is unchecked.  Default: 1,500 milliseconds.
Lock This Key to the Action	Check this check box to have Cisco Unity ignore additional input after callers press the key; Cisco Unity performs the action assigned to the key. To create efficient caller input menus, lock all keys except those that begin extensions on your system. You also can lock a key to block calls to extensions that begin with that key.  To lock the actions for all keys, uncheck the Allow Callers to Dial check box.  Default: Check box not checked.

Table 21-4 Call Management &gt; Call Handlers &gt; Caller Input Page (continued)

Field	Considerations
Action	<p>Indicate the action that Cisco Unity performs after a caller presses the corresponding key. For Cisco Unity to recognize caller input, the Allow Caller Input check box must be checked on the Greetings page.</p> <ul style="list-style-type: none"> <li>• Ignore Key—No action taken. Cisco Unity plays the entire greeting, then performs the after-greeting action.</li> <li>• Skip Greeting—Cisco Unity skips the greeting and performs the after-greeting action. Skip Greeting is assigned to # by default to provide callers a standard way to skip greetings.</li> <li>• Take Message—Cisco Unity records a message from the caller. The greeting should indicate that a message will be recorded. Click the Take Message link to view the associated Messages page.</li> <li>• Say Good-bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul> <p>Default: Ignore Key.</p>

## Call Handler Messages Settings

The messages settings specify who receives the messages for a call handler, the maximum recording length for messages from unidentified callers, what callers can do when leaving messages, and what happens to calls after messages are left. (Note that for some integrations, you can set up Cisco Unity so that as a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. To do so, see the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19.)

Use the following table to learn more about message settings.

**Table 21-5 Call Management > Call Handlers > Messages Page**

Field	Considerations
Message Recipient	<p>Select the subscriber or public distribution list that receives messages left for this call handler. Select a recipient type from the list, then click Select.</p> <p>When you select a public distribution list, each member of the list receives the call handler messages.</p> <p>Default: A selected subscriber.</p>
Maximum Message Length in Seconds	<p>Set the recording length allowed for messages left by unidentified callers.</p> <p>Recipients may want to limit the length of messages from unidentified callers. Some departments, such as Customer Service, may want to permit much longer messages.</p> <p>If enabled, a warning tone will sound before the maximum message length is reached.</p> <p>Default: 300 seconds.</p>
After Message Action	<p>Indicate the action that Cisco Unity performs after an unidentified caller leaves a message:</p> <ul style="list-style-type: none"> <li>• Say Good-bye—Cisco Unity plays a brief goodbye, and the call is disconnected. Click the Say Good-bye link to view the Goodbye call handler.</li> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory assistance.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul> <p>Default: Hang Up.</p>
Callers Can Edit Messages	<p>Check this check box to allow callers to be prompted to listen to, add to, rerecord, or delete their messages.</p> <p>Balance giving callers the additional control of editing messages with having voice messaging ports tied up for the additional time.</p> <p>Default: Check box checked.</p>
Mark Messages as Urgent	<p>Indicate the action that Cisco Unity will allow:</p> <ul style="list-style-type: none"> <li>• Always—All messages left by unidentified callers are marked urgent. This may be useful for Sales or Technical Support call handlers.</li> <li>• Never—Messages left by unidentified calls are never marked urgent.</li> <li>• Ask Caller for Their Preference—Cisco Unity asks unidentified callers whether to mark their messages urgent.</li> </ul> <p>Cisco Unity plays new urgent messages before other messages.</p> <p>Default: Never.</p>







## Directory Handler Settings

---

### Overview: Directory Handler Settings

Directory handlers provide directory assistance in Cisco Unity that callers can use to reach subscribers. When a caller searches on a subscriber name or part of a name, a directory handler looks up the extension and routes the call to the appropriate subscriber. Subscribers must have recorded names to be accessed by using directory handlers.

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.

The multiple directory handler feature provides quick, effective, and secure directory searches for systems with hundreds or thousands of subscribers. Multiple directory handlers are also used for call routing in headquarters and branch office deployments where Cisco Unity provides centralized call processing. Administrators can create as many directory handlers as they need to manage caller searches for subscribers.

See the following sections in this chapter for more information:

- [Creating and Modifying Directory Handlers, page 22-1](#)
- [Directory Handler Profile Settings, page 22-3](#)
- [Directory Handler Search Options Settings, page 22-5](#)
- [Directory Handler Match List Options Settings, page 22-6](#)
- [Directory Handler Caller Input Settings, page 22-8](#)

### Creating and Modifying Directory Handlers

You can use the default pre-defined Directory Handler or any other existing directory handler as a template to create additional directory handlers. Create as many directory handlers as needed to route calls to subscribers by using available filters such as location, class of service, and public distribution list membership.

You can also modify or delete directory handlers; however, note that the Default Directory handler can be modified, but not deleted.

Subscribers can be listed in more than one directory handler.

Because directory handlers do not have greetings, 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.

### To Create a Directory Handler

- 
- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Directory Handlers >** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Directory Handler dialog box, enter information as applicable in the Name field.
- Step 4** Select **New Handler** or **Based on Existing Handler**. If you select Based on Existing Handler, select the applicable directory handler in the Based On field.
- Note that if you base a new directory handler on an existing one, all of the settings are copied except extension and recorded name. If you select New Handler, the new directory handler is based on the default directory handler.
- Step 5** Click the **Add** button.
- Specify the settings for your new directory handler, as applicable, and then click the **Save** icon.
- Note that when directory handlers are based on Public Distribution Lists, there may be a delay in synchronizing and accessing new directory handlers by using the Cisco Unity phone conversation.
- 

Depending on the complexity of the Cisco Unity system configuration, synchronization of the new directory handler can take several minutes to several hours to complete. Factors that can affect synchronization speed include:

- System configuration, including multi-domain environments, organization unit structure, synchronization timer setting, and public distribution list complexity
- Cisco Unity Digital Networking configuration
- Number of subscribers and public distribution lists

When a directory handler is scoped by a distribution list, the membership is synchronized from the IBM Lotus Notes Directory into the Cisco Unity SQL database. Changing the distribution list by which the directory handler is scoped requires a synchronization. This synchronization takes place when the Cisco Unity directory services (AvDSAD and AvDSGlobalCatalog) poll the directory for any changes to be applied to the SQL database, which usually occurs within 15 to 20 minutes after the directory handler scope change is made in the Cisco Unity Administrator.

If an outside caller calls into Cisco Unity, and navigates to a recently created or modified directory handler on which synchronization has not yet completed, the Cisco Unity conversation may not present the full list of the directory members and/or may fail to find some directory members. This can also occur if the system administrator calls into Cisco Unity to verify directory handler additions or changes immediately after the changes are made in the Cisco Unity Administrator.

To initiate an immediate synchronization, do the following procedure.

### To Manually Synchronize the Cisco Unity Database

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page.
- Step 2** In the Replicate Cisco Unity directory objects section, click **Changed Objects**.
- The Settings page is refreshed and the database changes will be synchronized in the background.
- Step 3** Wait a few minutes, then call in to Cisco Unity and confirm that the subscriber(s) can be located in the directory handler.

- Step 4** If the subscriber(s) still can not be located, confirm that they have recorded names. Subscribers must have recorded names to be accessed by using directory handlers.
- 

#### To Modify a Directory Handler

---

- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Directory Handler** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the directory handler that you want to modify.
- Step 4** Change settings as applicable, and then click the **Save** icon.

Note that when the directory handler is based on a Public Distribution List, there may be a delay in synchronizing and accessing the changes by using the Cisco Unity phone conversation.

---

#### To Delete a Directory Handler

---

- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Directory Handler** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the directory handler that you want to delete.
- Step 4** Click the **Delete** icon.
- Step 5** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 6** In the left pane, under Diagnostic Tools, double-click **DBWalker**. (Running DBWalker ensures that any links to the deleted directory handler from other objects, such as call handlers, are identified.)
- Step 7** In the Options pane, check the following check boxes:
- Remove Orphaned Call Handlers**
  - Delete Empty Private Distribution Lists**
  - Set Broken User Keys to Ignore**
  - Remove References to Missing Greeting or Voice Name Wav Files**
- Step 8** In the Logging pane, enter the location for the output log file.
- Step 9** Click **Walk Database**.
- Step 10** Click **OK**, then click **OK** again to view the output log.
- Step 11** Click **Exit**.
- 

## Directory Handler Profile Settings

The profile settings specify who owns a directory handler, the extension (if any) that callers dial to reach the directory handler, and the language in which callers hear system prompts.

Use the following table to learn more about profile settings.

**Table 22-1 Call Management > Directory Handler > Profile Page**

Field	Considerations
Name	<i>Display only.</i> This setting shows the name of the selected directory handler.
Created	<i>Display only.</i> This setting shows the date and time that the directory handler was created.
Owner	This setting shows the directory handler owner. The owner can be any subscriber that has the authority to request changes to the directory handler. To change the owner, click Change. Default: Example Administrator.
Owner Type	A directory handler can only be owned by a subscriber.
Recorded Voice	This setting shows the recorded name of the directory handler.  To record the directory handler name, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.
Extension	Enter the extension, if any, that callers dial to reach the directory handler. When the directory handler is reached only from one-key caller input, do not enter an extension here.  Default: 555 or blank, depending on how the directory handler was created.
Language	Select the language in which Cisco Unity plays the handler system prompts. If you choose Inherited, Cisco Unity determines the language to use for system prompts on a per-call basis, depending on the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.  The default phone language and the list of languages shown here are set on the System > Configuration > Phone Languages page Default: Inherited.
Play All Names	Check the check box to play the names of subscribers in the directory for caller selection, rather than requiring the caller to search by spelled name.  Cisco Unity plays the names of all subscribers in the directory when either of the following conditions are true: <ul style="list-style-type: none"> <li>• One to five subscriber names are listed in the directory.</li> <li>• The caller chooses to play all names listed in the directory. When there are more than five (but less than 51) subscriber names listed in the directory, the Cisco Unity phone conversation allows callers the choice of either searching for a subscriber in the directory by spelled name or having Cisco Unity play all names listed in the directory.</li> </ul> When a directory handler includes more than 50 subscriber names, Cisco Unity requires the caller to search for a subscriber by spelled name.  When there are no subscriber names listed in the directory, Cisco Unity sends the caller to the call handler specified on the Caller Input page. Default: Check box not checked.

# Directory Handler Search Options Settings

The search options settings specify whether a directory handler searches for subscribers by using first name first, or last name first. Additionally, these settings allow you to restrict directory handler searches to the local Cisco Unity server, a public distribution list, a class of service, or if your organization uses Digital Networking to network Cisco Unity servers within a dialing domain, to expand searches to Cisco Unity servers at other locations. For more information on dialing domains, see the “Dialing Domains” section in the “Digital Networking” chapter of the *Networking in Cisco Unity Guide*. (The *Networking in Cisco Unity Guide* is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/net/net403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net403/dom/index.htm).)

Even if you have Digital Networking set up, you may want to consider limiting directory handler searches to the local server if either of the following conditions is true:

- If there are a large number of subscribers with the same name in your organization. In this situation, if you enable directory handler searches for multiple locations, the list of matching names presented to callers may be too long to be useful.
- If it is important to retain the individual call transfer settings for subscribers associated with other networked locations. If you enable directory handler searches for multiple locations, any calls transferred from a directory handler to subscribers not associated with the local server are automatically handled by the phone system—rather than by Cisco Unity—even if these subscribers are set up for supervised transfers on their own local Cisco Unity servers. As a result, the call screening, call holding, and announce features would not be available on these calls. See the “Subscriber Template Call Transfer Settings” section on page 13-9 for more information on call transfer types.

Use the following table to learn more about search option settings.

**Table 22-2 Call Management > Directory Handler > Search Options Page**

Field	Considerations
Search In	<p>Select the scope for directory handler searches:</p> <ul style="list-style-type: none"> <li>• Local Cisco Unity Server Only—Restricts directory handler searches to subscribers associated with the Cisco Unity server that the caller dialed.</li> <li>• Location—Restricts directory handler searches to subscribers associated with the primary and local delivery locations for the selected Cisco Unity server.</li> <li>• Class of Service—Restricts directory handler searches to subscribers associated with the selected Class of Service on the local Cisco Unity server.</li> <li>• Dialing Domain—Expands directory handler searches to include subscribers associated with other Cisco Unity servers within a dialing domain. Do not use this option if your organization has large numbers of subscribers with the same name at multiple locations or if it is important to retain call transfer settings for subscribers who are not associated with the local Cisco Unity server. Instead, choose Local Unity Server Only, a Public Distribution List, or a Class of Service.</li> <li>• Public Distribution List—Restricts directory handler searches to subscribers associated with the selected Public Distribution List. Note that all Public Distribution Lists are presented, including lists that may contain Cisco Unity subscribers who do not have recorded names (and thus will not be presented to callers), and/or lists that may contain members who are not Cisco Unity subscribers.</li> </ul> <p>Provide information in the call handler greeting that routes callers to this directory handler, explaining how callers can contact other Cisco Unity locations.</p> <p>Default: Local Cisco Unity Server Only.</p>
Search By	<p>Select the method that callers use to spell a subscriber name:</p> <ul style="list-style-type: none"> <li>• First Name, Last Name—For example, callers press 535 (KEL) to reach Kelly Bader.</li> <li>• Last Name, First Name—For example, callers press 223 (BAD) to reach Kelly Bader.</li> </ul> <p>Include instructions that reflect the Search By selection in the call handler greeting that routes callers to this directory handler.</p> <p>Default: Last Name, First Name.</p>

## Directory Handler Match List Options Settings

The match list options settings specify whether, on a unique match, Cisco Unity routes the caller to the extension automatically, or first asks the caller to confirm the match. This page also specifies how Cisco Unity presents directory matches to callers—either by stating the extensions (“for Pat Amos, press 123; for Gerry Anderson, press 234...”) or by offering a menu of choices (“for Pat Amos, press 1; for Gerry Anderson, press 2...”).

Use the following table to learn more about match list options settings.

**Table 22-3 Call Management > Directory Handler > Match List Options Page**

Field	Considerations
On a Unique Match	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Route Automatically—Cisco Unity routes the call to the extension assigned to the subscriber without prompting the caller to verify the match.</li> <li>• Request Caller Input First—Cisco Unity prompts the caller to verify the match.</li> </ul> <p>Default: Request Caller Input First.</p>
Announce Matched Names Using	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Extension Format—Cisco Unity announces the names and extensions of matching subscribers. For example, “For Pat Amos, press 123. For Gerry Anderson, press 104.” Callers enter the extension number to choose a subscriber. <p>The Play All Names option on the Directory Handler &gt; Profile Page is not supported for use with Extension Format. If the Play All Names check box is checked when Extension Format is selected, and when Cisco Unity plays all names listed in the directory (rather than the caller searching for a subscriber by spelled name) Cisco Unity announces the names of matching subscribers, but not their extensions. For example, “Pat Amos. To repeat, press 1. To choose the name, press 2. To go to the next name, press #.”</p> </li> <li>• Menu Format—Cisco Unity provides a menu of subscribers. For example, “For Pat Amos, press 1. For Gerry Anderson, press 2.” Callers enter the menu number to choose a subscriber. <p>When Menu Format is selected in combination with the following fields, Cisco Unity provides three different menu options:</p> <ul style="list-style-type: none"> <li>– When the Play All Names check box is checked on the Directory Handler &gt; Profile page, and when Cisco Unity plays all names listed in the directory (rather than the caller searching for a subscriber by spelled name), Cisco Unity plays the names of subscribers in the directory for caller selection, rather than requiring the caller to search by spelled name. For example, “Pat Amos. To repeat, press 1. To choose the name, press 2. To go to the next name, press #.”</li> <li>– When the Announce Extension with Each Name check box is checked, and when Cisco Unity plays all names listed in the directory (rather than the caller searching for a subscriber by spelled name), Cisco Unity provides a menu of subscribers that includes subscriber extensions. For example, “For Pat Amos at extension 123, press 1. For Gerry Anderson at extension 104, press 2.”</li> <li>– When the Announce Extension with Each Name and Play All Names check boxes are checked, Cisco Unity provides a menu of subscribers that includes subscriber extensions. For example, “Pat Amos at extension 123. To repeat, press 1. To choose the name, press 2. To go to the next name, press #.”</li> </ul> </li> </ul> <p>Default: Menu Format.</p>

**Table 22-3 Call Management > Directory Handler > Match List Options Page (continued)**

Field	Considerations
Announce Extension with Each Name	<p>Cisco Unity provides a menu of subscribers that includes subscriber extensions. Callers enter the menu number to select a subscriber. For example, “For Pat Amos at extension 123, press 1. For Gerry Anderson at extension 104, press 2.” Callers might take note of subscriber extensions to skip directory assistance the next time they call.</p> <p>This functionality is supported only when Menu Format is selected in the Announce Matched Names Using field.</p> <p>Default: Check box checked.</p>

## Directory Handler Caller Input Settings

The caller input settings specify the number of seconds a directory handler waits for caller input, the number of times the caller is prompted to spell a name, and the action that Cisco Unity takes if the caller exits a directory handler.

Use the following table to learn more about caller input settings.

**Table 22-4 Call Management > Directory Handler > Caller Input Page**

Field	Considerations
Timeout if No Input in Seconds	<p>Enter the number of seconds that Cisco Unity waits for caller input. When the caller does not press any key, Cisco Unity asks for confirmation that the caller is still there. If there is no response, Cisco Unity performs the action selected in the If Caller Exits Send To field.</p> <p>Default: Five seconds.</p>
Timeout After Last Input in Seconds	<p>Enter the number of seconds that Cisco Unity waits after caller input before performing the action indicated by the input.</p> <p>Default: Four seconds.</p>
Times to Repeat Name Entry Prompt	<p>Enter the number of times to reprompt the caller for input. When the caller does not press any key after being reprompted, Cisco Unity asks for confirmation that the caller is still there. If there is no response, Cisco Unity performs the action selected in the If Caller Exits Send To field.</p> <p>Default: One time.</p>

**Table 22-4 Call Management > Directory Handler > Caller Input Page (continued)**

Field	Considerations
If Caller Exits Send To	<p>Select the destination to which calls are sent if the caller exits the directory handler by pressing * or by not responding to prompts:</p> <ul style="list-style-type: none"> <li>• Call Handler—Sends the call to another call handler that you select.</li> <li>• Directory Handler—Sends the call to another directory handler that you specify.</li> <li>• Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>• Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>• Interview Handler—Sends the call to the interview handler that you select.</li> <li>• Sign-In—Sends the call to the subscriber logon conversation.</li> <li>• Subscriber—Sends the call to the subscriber that you select.</li> </ul> <p>Default: Call Handler.</p>





## Interview Handler Settings

---

### Overview: Interview Handler Settings

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 stops recording either when the response reaches the maximum recording time that you have specified, or when the caller stops speaking. Cisco Unity 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.

By default, this recipient is the Example Administrator. If you want these messages to be routed to another recipient, choose a subscriber (such as the operator) or a distribution list as the recipient. Do not delete the Example Administrator account unless you have assigned the applicable subscriber(s) or public distribution list(s) to review the messages sent to the Interview call handler. In addition, note that if you later delete the assigned subscribers or distribution lists, Cisco Unity does not prompt you to assign a replacement.

### About the Example Interview Handler

Cisco Unity comes with a predefined interview handler called Example Interview, which you can modify but not delete. You can have callers routed to this interview handler if they do not press any phone keys during the Opening Greeting, or by selecting it as the after-greeting action on the Greetings page of the call handler that plays the Opening Greeting.

The Example Interview handler asks the following questions:

- What person or department are you trying to reach?
- What is your name?
- What is your phone number?
- What are the best times to reach you?
- Is there any other information you would like to leave?

See the following sections in this chapter for more information about interview handlers:

- [Creating and Modifying Interview Handlers, page 23-2](#)
- [Interview Handler Profile Settings, page 23-2](#)

- [Interview Handler Questions Settings, page 23-4](#)

## Creating and Modifying Interview Handlers

You can modify the Example Interview handler, and you can create new ones.

### To Create a New Interview Handler

- 
- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Interview Handler** page.
  - Step 2** Click the **Add** icon.
  - Step 3** In the Add an Interview Handler dialog box, enter information as applicable in the Name field.
  - Step 4** Select **New Interview Handler** or **Based on Existing Interview Handler**. If you select Based on Existing Interview Handler, select the applicable interview handler in the Based On field.
  - Step 5** Click the **Add** button.
  - Step 6** Enter settings for your new interview handler, and then click the **Save** icon.
- 

### To Modify an Interview Handler

- 
- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Interview Handler** page.
  - Step 2** Click the **Find** icon.
  - Step 3** Double-click the interview handler that you want to modify.
  - Step 4** Change settings as applicable, and then click the **Save** icon.
- 

## Interview Handler Profile Settings

The profile settings specify to whom the interview response is delivered, the extension (if any) that callers dial to reach the interview handler, and the language in which callers hear system prompts.

Use the following table to learn more about profile settings.

**Table 23-1** *Call Management > Interview Handler > Profile Page*

Field	Considerations
Name	This displays the name of the interview handler. To change the name of the interview handler, enter a new name here, and then click the Save icon.
Owner	This setting displays the owner of the interview handler. The owner can be any subscriber or public distribution list that has the authority to request changes to the interview handler. Note that the owner is not necessarily the message recipient.  To change the owner, select an Owner Type and click Change.
Created	<i>Display only.</i> This setting shows the date and time the interview handler was created.

**Table 23-1 Call Management > Interview Handler > Profile Page (continued)**

Field	Considerations
Recorded Voice	<p>This is the recorded name of the interview handler.</p> <p>To record an interview handler name, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.</p>
Extension	<p>Enter the extension, if any, that callers can dial to reach the interview handler. If the interview handler is reached only from one-key caller input, do not enter an extension here.</p> <p>Default: Blank.</p>
Language	<p>Select the language in which Cisco Unity plays the handler system prompts. If you choose Inherited, Cisco Unity determines the language to use for system prompts on a per-call basis, depending on the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.</p> <p>The default phone language and the list of languages shown here are set on the System &gt; Configuration &gt; Phone Languages page.</p> <p>Default: Inherited.</p>
Deliver Response To	<p>Click Change and select a subscriber or public distribution list from the list. The subscriber or distribution list will receive messages left for this interview handler.</p> <p>Default: Subscriber.</p>
Response Urgency	<p>Select the urgency for the interview message. If you select Ask Caller, Cisco Unity asks callers if they want to mark the interview message urgent.</p> <p>Default: Mark Normal.</p>
After Interview Action	<p>Indicate the action that Cisco Unity performs after an unidentified caller leaves an interview message:</p> <ul style="list-style-type: none"> <li>• Send Caller To—Cisco Unity sends the call to the destination that you select: <ul style="list-style-type: none"> <li>– Call Handler—Sends the call to the call handler that you select.</li> <li>– Directory Handler—Sends the call to directory handler that you specify.</li> <li>– Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>– Hang Up—Disconnects the call. Use carefully; unexpected hang-ups can appear rude to callers.</li> <li>– Interview Handler—Sends the call to the interview handler that you select.</li> <li>– Sign-In—Sends the call to the subscriber logon conversation.</li> <li>– Subscriber—Sends the call to the subscriber that you select.</li> </ul> </li> </ul> <p>Default: Call Handler.</p>

## Interview Handler Questions Settings

You can record the questions for the interview handler on the Call Management > Interview Handler > Questions page. You can also specify the maximum recording length for caller responses. (Note that for some integrations, you can set up Cisco Unity so that as a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. To do so, see the [“Setting a Warning Tone for End of Recording”](#) section on page 28-19.)

Use the following table to learn more about interview handler question settings.

**Table 23-2** Call Management > Interview Handler > Questions Page

Field	Considerations
Question	Select the question number. The settings on the rest of the page apply to the question number selected here. Default: Default questions one through five.
Question Text	Enter the complete text of the selected question, if it is short, or a summarized version of the question, if it is long.
Maximum Message Length in Seconds	Enter the recording length, in seconds, allowed for caller responses to the selected question. If enabled, a warning tone will sound before the maximum message length is reached. Default: 30 seconds.
Recording	Record the interview question. To record the question, use the Media Master control bar. Use the Paste From File option on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording. Note that the Media Master is not available across a firewall.



## Call Routing

### Overview: Call Routing Tables

Call routing tables are used to route incoming calls to the operator or to specific subscribers, call handlers, directory handlers, or interview handlers. In addition, call routing tables are used to route subscribers to the subscriber logon conversation.

Cisco Unity has two call routing tables—one for direct calls and one for forwarded calls—that handle calls from subscribers and from unidentified callers. (Unidentified callers include both external callers and any callers calling Cisco Unity from an internal extension that is not associated with a subscriber account, such as a conference room.) 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 appropriately.

#### Direct Calls Call Routing Table

The Direct Calls call routing table handles calls from subscribers and unidentified callers that are dialed directly to Cisco Unity.

The predefined routing rules for the Direct Calls call routing table are:

- Attempt Sign-In—Calls from subscribers are routed to the subscriber logon conversation.
- Default Call Handler—Calls from unidentified callers are routed to the Opening Greeting.

#### Forwarded Calls Call Routing Table

The Forwarded Calls call routing table handles calls that are forwarded to Cisco Unity from either a subscriber extension or an extension that is not associated with a subscriber account (such as a conference room). The predefined routing rules for the Forwarded Calls call routing table are:

- Attempt Forward to Greeting—All calls forwarded from a subscriber extension are routed to the subscriber greeting.
- Default Call Handler—Calls forwarded from an extension that is not associated with a subscriber account are routed to the Opening Greeting.

You can change the order of the Attempt Sign-In and Attempt Forward to Greeting rules in the respective routing tables, but the Default Call Handler rule is always the last entry for both tables. You cannot modify or delete the predefined rules.

See the following sections in this chapter for more information:

- [How Call Routing Rules Work, page 24-2](#)
- [Creating and Modifying Call Routing Rules, page 24-3](#)

- [Direct Calls and Forwarded Calls Routing Table Settings, page 24-4](#)

## How Call Routing Rules Work

Call routing tables consist of a series of rules that let you route incoming calls based on the information that Cisco Unity 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 Cisco Unity receives a call, it first determines if it is a direct or forwarded call based on the information contained in the serial or DTMF packet sent by the phone system, and then applies the applicable call routing table. If the call information matches all of the settings for the first rule, the call is routed as specified in the rule. If any call information does not match the settings specified in the first rule, the call information is then compared to the settings 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 Cisco Unity 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 the call is received.

To set up routing rules correctly, you need to know what information your integration provides. Refer to the Call Information section in the Cisco Unity integration guide for your phone system for this information. You can also use the Cisco Unity Call Viewer to see the types of call information that your integration provides to Cisco Unity for inbound calls. To access the Call Viewer, on the Cisco Unity server desktop, double-click the Cisco Unity Tools Depot icon. In the left pane of the Tools Depot window, in the Switch Integration Tools directory, double-click Call Viewer.

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

### Example 1

In [Table 24-1](#), 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 will be routed to the Opening Greeting, according to the Default Call Handler rule.

**Table 24-1** Direct Calls Call Routing Table

Rule	Status	Call Type	Port	Trunk	Dialed Number	Calling Number	Schedule	Send Call To	Language
Operator	On	External calls	Any	Any	Any	Any	Weekdays	Attempt transfer for operator	Inherited
Attempt Sign-in	On	Both	Any	Any	Any	Any	Always	Attempt Sign-in	English
Default Call Handler	On	Both	Any	Any	Any	Any	Always	Attempt transfer for Opening Greeting	Inherited

### Example 2

In [Table 24-2](#), 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 24-2 Forwarded Calls Call Routing Table

Rule	Status	Call Type	Forwarding Station	Dialed Number	Calling Number	Schedule	Send Call To	Language
Customer Service	On	Both	5678	Any	Any	Always	Attempt transfer for Customer Service	Inherited
Product Info	On	Both	1234	Any	Any	Always	Send to greeting for Product Info	English
Attempt Forward	On	Both	Any	Any	Any	Always	Attempt Forward	English
Default Call Handler	On	Both	Any	Any	Any	Always	Attempt transfer for Opening Greeting	Inherited

## Creating and Modifying Call Routing Rules

Although you cannot modify the predefined routing rules in the Direct Calls and Forwarded Calls call routing tables, you can create additional call routing rules for each call routing table and modify them as needed.

### To Create a Call Routing Rule

- Step 1** In the Cisco Unity Administrator, for direct calls, go to the **Call Management > Call Routing > Direct Calls** page. For forwarded calls, go to the **Call Management > Call Routing > Forwarded Calls** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Call Routing Rule dialog box, enter the name of the new rule in the Name field.
- Step 4** Click the **Add** button.
- Step 5** Specify the settings for your new call routing rule, as applicable, and then click the **Save** icon. For more information about settings, see the [“Direct Calls and Forwarded Calls Routing Table Settings” section on page 24-4](#).

When you create a new rule, you only need to specify the criteria that will be 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.

### To Modify a Call Routing Rule

- Step 1** In the Cisco Unity Administrator, for direct calls, go to the **Call Management > Call Routing > Direct Calls** page. For forwarded calls, go to the **Call Management > Call Routing > Forwarded Calls** page.
- Step 2** In the routing table, click the rule that you want to modify.
- Step 3** Change settings as applicable in the fields above the table, and then click the **Save** icon.

# Direct Calls and Forwarded Calls Routing Table Settings

Use the following table to learn more about settings for call routing rules.

**Table 24-3** Call Management > Call Routing > Direct Calls and Forwarded Calls Pages

Field	Considerations
Rule Name	Enter a rule name. Rule names can be words or numbers. You might want the name to reflect the purpose of the rule (for example, “Sales menu”).
Status	Select one of the following settings: <ul style="list-style-type: none"> <li>Enabled—The routing rule is active and Cisco Unity will acknowledge all settings.</li> <li>Disabled—The routing rule is inactive and Cisco Unity ignores all settings within the rule.</li> </ul> Default: Enabled.
Call Type	Click the applicable Call Type, either Internal Calls or External Calls. To have the rule apply to all call types, click Both. Internal calls are from subscribers, and external calls are from unidentified callers. <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To. Your integration may not support this option.</p> Default: Both.
Ports (Direct Calls page only)	Enter the port number to have the rule apply to the port on which a call arrives. To set a consecutive range of ports, enter a hyphen between the port numbers (for example, 1–4). To set a list of ports, enter a comma between the ports (for example, 1,2,4). To have the rule apply to calls on all ports, enter * or leave the box blank. <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To.</p> Default: Blank.
Trunks (Direct Calls page only)	Enter the trunk number to have the rule apply to the trunk on which a call arrives. To set a consecutive range of trunks, enter a hyphen between the trunk numbers (for example, 1–4). To set a list of trunks, enter a comma between the trunk numbers (for example, 1,2,4). To have the rule apply to calls on all trunks, enter * or leave the box blank. <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To. Your integration may not support this option.</p> Default: Blank.
Forwarding Station (Forwarded Calls page only)	Enter the extension (station) to have the rule apply to the extension from which a call was forwarded. To have the rule apply to all extensions, enter * or leave the field blank. The * is a wildcard and can be used alone or with other numbers (for example, enter 2* to route all calls from any extension that begins with 2). <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To. Your integration may not support this option.</p> Default: Blank.

**Table 24-3 Call Management > Call Routing > Direct Calls and Forwarded Calls Pages (continued)**

Field	Considerations
Dialed Number (DNIS)	<p>Enter the phone number to have the rule apply to a number that callers dial to reach your organization. To have the rule apply to all numbers dialed, enter * or leave the box blank. The * is a wildcard and can be used alone or with other numbers (for example, enter 800* to control routing of all calls to 800 numbers).</p> <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To. Your integration may not support this option.</p> <p>Default: Blank.</p>
Calling Number (ANI)	<p>Enter the phone number to have the rule apply to a phone number from which calls originate. To have the rule apply to all originating phone numbers, enter * or leave the box blank. The * is a wildcard and can be used alone or with other numbers (for example, enter 212* to control routing of all calls from that area code).</p> <p>When a call matches all settings for the rule, the call is routed as specified in Send Call To. Your integration may not support this option.</p> <p>Default: Blank.</p>
Schedule	<p>Select a schedule to apply to this call routing rule. When a call arrives during the standard (open) hours of the selected schedule, and the call matches all other settings for the rule, the call is routed as specified in Send Call To.</p> <p>To have the rule apply 24 hours a day, seven days a week, click Always.</p> <p>To have different rules for standard and closed hours, create a rule with a selected schedule, followed by a rule set with Always.</p> <p>Default: Always.</p>
Language	<p>Select the language to be associated with the call. If you choose Inherited, Cisco Unity determines the language to use on a per-call basis, depending on the handler or routing rule that processed the call. If the language is set to Inherited for every rule and handler that processes a call, then the system prompts are played in the default phone language.</p> <p>If your organization has purchased additional language licenses, routing rules can also be used to change the language in which Cisco Unity plays system prompts to callers. For example, you could route calls and set the language for the system prompts based on the dialed number, so that different callers can hear identical information but in different languages.</p> <p>The list of languages shown here is set on the System &gt; Configuration &gt; Phone Languages page.</p> <p>Default: Inherited.</p>

Table 24-3 Call Management &gt; Call Routing &gt; Direct Calls and Forwarded Calls Pages (continued)

Field	Considerations
Send Call To	<p>Select one of the following destinations for a call that matches all settings for the rule:</p> <ul style="list-style-type: none"> <li>• Attempt Forward—Forwards the call if the forwarding station belongs to a subscriber. The calling number is used as the ID, and if the extension is found, the call is forwarded to the subscriber greeting. If the extension is not found, the next rule in the routing table is applied to the call information.</li> <li>• Attempt Sign-In—Sends the call to the subscriber logon conversation, if the calling number belongs to a subscriber. The calling number is used as the ID. If the call is not from a subscriber, the next rule in the routing table is applied to the call information.</li> <li>• Call Handler—Sends the call to the call handler that you select.</li> <li>• Directory Handler—Sends the call to the directory handler that you select.</li> <li>• Greetings Administrator—Sends the call to a conversation for changing call handler greetings over the phone.</li> <li>• Interview Handler—Sends the call to the interview handler that you select.</li> <li>• Sign-In—Sends the call to the subscriber logon conversation, which prompts the caller to enter an ID.</li> <li>• Subscriber—Sends the call to the subscriber that you select.</li> </ul> <p>Defaults: Attempt Forward for Forwarded Calls, Directory Handler for Direct Calls.</p>
Routing Table	<p><i>Display only.</i> This setting shows the call routing rules for direct calls or for forwarded calls. The order of the rules is important. Cisco Unity compares a call to each rule in the order specified in the table from the top down until it finds a match. The first rule that matches a call determines where the call is routed.</p>



## Restriction Tables

### Overview: Restriction Tables

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

- Transferring calls.
- Recording and playback by phone from Cisco Unity applications when the phone is the designated recording and playback device in the Media Master, or in the VCR-style player/recorder available in Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity. (The Media Master is available in the Cisco Unity Administrator and the Cisco Unity Assistant.)
- Delivering faxes to a fax machine.
- Sending message notifications.

For example, you can specify that subscribers 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 subscriber or administrator accesses Cisco Unity.

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.

### Predefined Restriction Tables

Cisco Unity 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.

<b>{Default Outdial}</b>	Restricts numbers for message notifications. Also restricts the subscriber extensions that Cisco Unity dials when the phone is selected as the recording and playback device in the Media Master or the VCR-style player/recorder available in Lotus Notes with DUCS for Cisco Unity. (The Media Master is available in the Cisco Unity Administrator and the Cisco Unity Assistant.)
<b>{Default Transfer}</b>	Restricts numbers for call transfers.
<b>{Default Fax}</b>	Restricts numbers for fax delivery.

See the following sections in this chapter for more information:

- [How Restriction Tables Work, page 25-2](#)
- [Creating and Modifying Restriction Tables, page 25-3](#)
- [Restriction Table Settings, page 25-4](#)

## How Restriction Tables Work

When a subscriber uses the Cisco Unity Assistant or the Cisco Unity conversation to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer, Cisco Unity applies the applicable restriction table to verify that the phone number entered is allowed. The same thing happens when an administrator uses the Cisco Unity Administrator to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer. In each case, the restriction table used is the one associated with the subscriber or administrator who is changing the number. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

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

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 matching the call pattern are permitted for use. The restriction table is applied when a subscriber or an administrator attempts to change a number controlled by a restriction table, not when Cisco Unity tries to complete a transfer or delivery.

When a restriction table is applied to a number (such as a pager number for a message notification), Cisco Unity 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, Cisco Unity then compares the number with the call pattern in the second dial string, and so on, until it finds a match. When Cisco Unity finds a match, it either permits or restricts the use of this 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 [Figure 25-1](#) restricts most long distance phone numbers, but permits extensions starting with “91.” In this case, if a subscriber enters “9123” as a transfer number, Cisco Unity 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, Cisco Unity 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, Cisco Unity 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, Cisco Unity permits this number to be used.

Figure 25-1 Example 1

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

The restriction table in Figure 25-2 restricts long distance phone numbers and numbers less than four digits long. 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 less 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.

Figure 25-2 Example 2

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

## Creating and Modifying Restriction Tables

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 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. It prevents a case in which the entered number does not match any call pattern in the table. However, you can change the Allow This String field setting for this dial string to either permit or restrict a number.

### To Create a New Restriction Table

- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Restriction Tables** page.
- Step 2** Click the **Add** icon.

- Step 3** In the Add a Restriction Table dialog box, enter information as applicable in the Name field.
- Step 4** Select **New Restriction Table** or **Based on Existing Restriction Table**. If you select Based on Existing Restriction Table, select the applicable restriction table in the Based On field.
- Step 5** Click the **Add** button.
- Step 6** Enter settings for your new restriction table, and then click the **Save** icon.

---

### To Modify a Restriction Table

- Step 1** In the Cisco Unity Administrator, go to any **Call Management > Restriction Tables** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the restriction table that you want to modify.
- Step 4** Do one of the following:
- To add a dial string, click **Add Dial String** and enter settings for the new dial string as applicable.
  - To delete a dial string, click the dial string number in the table at the bottom portion of the Restriction Tables page, and then click **Remove Dial String**.
  - To modify a dial string, click the dial string number in the table at the bottom portion of the Restriction Tables page, and change settings as applicable.
- Step 5** Click the **Save** icon.
- 

## Restriction Table Settings

Use the following table to learn more about settings for restriction tables.

**Table 25-1** *Call Management > Restriction Tables Page*

Field	Considerations
Restriction Table Name	Enter a descriptive name for the types of phone numbers that are restricted or for the types of subscribers to which the restrictions apply.
Minimum Digits Allowed	Enter the minimum number of digits—including access codes—in a call transfer, message notification, or fax delivery number, in order for Cisco Unity to apply the restriction table to the number. Numbers containing fewer digits are automatically permitted.  For example, to permit subscribers to use four-digit numbers, enter 5 in the Minimum Digits Allowed field. Enter 1 (the default value) to apply the restriction table to as many digits as the subscriber enters.

Table 25-1 Call Management &gt; Restriction Tables Page (continued)

Field	Considerations
Maximum Digits Allowed	<p>Enter the maximum number of digits—including access codes—in a call transfer, message notification, or fax delivery number permitted by the restriction table. Numbers containing more than the maximum digits are automatically restricted.</p> <p>For example, if local calls in your area are seven digits long, and you want to prevent subscribers from using long distance phone numbers, enter 8 as the maximum digits permitted (“8” is the length of local numbers, including the external access code for the phone system).</p> <p>Default: 30 digits.</p>
Selected Dial String	<p><i>Display only.</i> This setting identifies the dial string in the restriction table that is selected for modifying.</p> <p>If you click the Add Dial String button, the new dial string is always added to the first row of the restriction table as Dial String 0. Up to 100 dial strings can be specified in a table.</p> <p>Note that the order of the dial strings is very important. Cisco Unity 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 permitted or restricted according to the first call pattern it matches.</p>
Allow This String	<p>Select the action that Cisco Unity takes when a number matches a call pattern:</p> <ul style="list-style-type: none"> <li>• Yes—Permit use of phone numbers matching the pattern.</li> <li>• No—Do not permit use of phone numbers matching the pattern.</li> </ul> <p>Default: No.</p>
Call Pattern	<p>Enter specific numbers or patterns of numbers that can be permitted or restricted. Include external and long-distance access codes. Use digits 0 through 9 and the following special characters:</p> <ul style="list-style-type: none"> <li>• * to match zero or more digits.</li> <li>• ? to match exactly one digit. Each ? serves as a placeholder for one digit.</li> <li>• # to correspond to the # key on the phone.</li> </ul> <p>Default: No long distance, no international numbers.</p>





## Reports

---

### Overview: Reports

You can use Cisco Unity reports to gain information about subscribers and system activity. Some Cisco Unity reports provide information about subscribers and system activity over a period of time. Others offer a “snapshot” of a particular Cisco Unity entity as it stands at the time you run the report.

See the following sections in this chapter to learn more about using Cisco Unity reports:

- [About Report Data, page 26-2](#)—This section provides information about how Cisco Unity gathers and stores report data, and which settings you can change to ensure that your reports contain the data you need.
- [Generating Reports, page 26-2](#)—This section details how to generate, view, and print Cisco Unity reports.

See the following sections in this chapter for information on specific reports:

#### Subscriber Reports

- [Subscribers Report, page 26-4](#)—This report includes profile and account information about each subscriber.
- [Subscriber Message Activity Report, page 26-4](#)—This report shows when subscriber messages were left and when they were accessed.
- [Distribution Lists Report, page 26-5](#)—This report shows the owner, members, and creation date of public distribution lists.
- [Failed Login Report, page 26-5](#)—This report shows details of failed attempts to log on to subscriber accounts (by phone) and to the Cisco Unity Administrator.
- [Transfer Billing Report, page 26-6](#)—This report provides information about call transfers from call handlers and subscribers; this information can be used for billing purposes.
- [Outcall Billing Report, page 26-7](#)—This report provides information about outgoing calls made by Cisco Unity for message notifications; this information can be used for billing purposes.

#### System Reports

- [Administrative Access Activity Report, page 26-8](#)—This report shows details of all changes entered into the Cisco Unity Administrator; this information can be used as an audit trail of commands entered by system administrators.
- [Event Log Report, page 26-9](#)—This report provides information from the Windows application log.

- [Port Usage Report, page 26-9](#)—This report shows activity on each port; this information can be used to determine when to add new ports.
- [System Configuration Report, page 26-10](#)—This report provides information on system resource allocation.
- [Unresolved References Report, page 26-11](#)—This report shows any call handlers that were left in an invalid state when the Cisco Unity Administrator was not used to delete subscriber accounts.
- [Call Handler Traffic Report, page 26-11](#)—This report shows how many calls are routed through a particular call handler and how callers are choosing to exit that handler.

## About Report Data

Cisco Unity reports that provide information about subscribers and system activity over a period of time contain log-based data. For example, the Call Handler Traffic report shows how many calls are routed through a particular call handler and how callers are choosing to exit that handler during the time period that you specify. Other Cisco Unity reports offer a “snapshot” of subscriber or system data as it stands at the time you run the report, and therefore they reflect the current status of a particular Cisco Unity entity.

Cisco Unity automatically gathers and stores data that is used in log-based reports every 30 minutes. You specify how long Cisco Unity stores the data in the Cleanup Interval for Logger Data Files in Days field on the System > Configuration > Settings page. For example, if you have set this field to three, a log-based report will reflect activity only for the last three days, even if you specified more than three days in the time range for the report.

By default, Cisco Unity deletes report files every seven days. To change how often reports are deleted, adjust the settings for the Cleanup Interval for Report Files in Days field on the System > Configuration > Settings page.

## Generating Reports

When you generate a report, you can specify some or all of the following:

- The subscribers, administrators, or distribution lists to include in the report
- The date and time range to include
- The sort order for the data in the report

You also choose to save the report either as a Web page or as a comma-delimited file:

<b>Web page</b>	An HTML file. You use a Web browser to view and to print the report. In some cases, a report may be too large to be viewed in a Web browser.
<b>Comma-delimited file</b>	A text file (also known as a comma separated or CSV file). Each row in the report appears on a separate line, and values are separated by commas. Select this format if you want to view or print the information in another application, for example, a spreadsheet program.

The best time to generate reports is when the system is not busy: after regular business hours when Cisco Unity is not processing many calls, or when there are no other processes running (for example, before or after a full backup). Note that for large systems, reports that offer a “snapshot” of subscriber or system data may take a significant amount of time to run.

In the current release of Cisco Unity, reports cannot be scheduled in advance, and if you turn off Cisco Unity while there are reports in the report queue, the reports will be deleted.

## Viewing and Printing Reports

When a report has completed, the name of the output file is displayed on the Reports page of the Status Monitor. To access the report file, all Cisco Unity administrators must have full read/write access and all Domain Users must have read rights to the CommServer\Reports directory located on the Cisco Unity server (these access levels are set by default). To have read rights, an administrator or user must either be a member of the domain that Cisco Unity is in or be associated with a domain that is trusted by the domain that Cisco Unity is in.

All reports contain a report header followed by columns of data. If, for example, you generate a report for all subscribers, the subscriber name is included above the data associated with the subscriber.

### To View a Report

---

- Step 1** Monitor the completion status of the report in the Reports page of the Status Monitor. When the report has completed, note the name of the report output file.
  - Step 2** Go to the CommServer\Reports directory. Locate the report output file to be viewed.
  - Step 3** If the report is in Web page format, the browser will start automatically and display the information. If the report is in comma-delimited format, you may be required to choose an application in which to display the information.
- 

### To Print a Report

---

- Step 1** View the report, as described in the “[To View a Report](#)” procedure.
  - Step 2** On the File menu, click **Print**.
- 

### To View the Status of a Report

The ability to view report status is controlled by class of service.

---

- Step 1** Go to **http://<Cisco Unity server name>/status**, or double-click the desktop shortcut to the Status Monitor.
  - Step 2** Click **Reports**.
-

## Subscribers Report

Use the Subscribers report to get a list of Cisco Unity subscribers. You can generate the report for an individual subscriber or for all Cisco Unity subscribers.

The Subscribers report includes the following information:

<b>First Name, Last Name</b>	The name of the subscriber for which the report was generated. Note that the distribution list selection option is not supported in this release.
<b>Alias</b>	The subscriber short name.
<b>Location</b>	The Cisco Unity location.
<b>Domain</b>	The Windows domain name assigned to a subscriber. This field contains no data when the report is run on a Domino mailstore.
<b>Billing ID</b>	The billing ID of a subscriber.
<b>Class of Service (COS)</b>	The class of service assigned to a subscriber.
<b>Extension</b>	The primary phone extension assigned to a subscriber. Alternate extensions are not listed.
<b>Inbox Size</b>	The total size, in kilobytes, of all e-mail, voice, and fax messages stored for the subscriber.

## Subscriber Message Activity Report

Use the Subscriber Message Activity report to diagnose voice message problems reported by a subscriber (for example, voice messages are not being sent or received, or the message waiting indicator is not being turned on or off properly). You generate this report for an individual subscriber only.

The Subscriber Message Activity report includes the following information:

<b>Date and Time</b>	The date and time that the subscriber took action on the message.
<b>Source</b>	Either the computer or the phone that generated the message activity.
<b>Action Taken in Response to Message</b>	The activity that took place in regards to voice messages (for example, New Message, Message Read, Save, Delete, Mark New, Login, and Logoff). The actions MWI On Requested and MWI On Completed indicate, respectively, that Cisco Unity sent a request to the phone system to turn on the MWI and received a request-completed confirmation. In cases where the phone system does not provide a confirmation, Cisco Unity assumes the request was successful.
<b>Number of New Messages</b>	The number of new voice messages in the subscriber mailbox.
<b>Sender's Name and DTMF</b>	The name and extension of the message sender, if known.
<b>Date and Time Message Arrived</b>	The date and time the message arrived in the mailbox.

<b>Dial Out Number</b>	The number to which a message notification was sent.
<b>Dial Out Result</b>	The result of the outgoing call for the message notification. Possible results include: <ul style="list-style-type: none"> <li>• Busy—The dialed number was busy.</li> <li>• Connected—The called party answered the phone.</li> <li>• Failure—The call failed.</li> <li>• Port Disabled—All ports for outgoing calls were disabled.</li> <li>• Port Unavailable—No ports were available for the outgoing call.</li> <li>• RNA (Ring No Answer)—The dialed number did not answer.</li> <li>• Release—The result is unknown. This typically happens for notifications sent to pagers.</li> <li>• Unknown—The result is unknown.</li> </ul>

## Distribution Lists Report

Use the Distribution Lists report to get a listing of all public distribution lists and, optionally, the members in each list. You can generate the report for a selected public distribution list or for all public distribution lists.

If you want the report to include the names of distribution list members, check the List All Members For Each Distribution List check box.

The Distribution Lists report includes the following information:

<b>Creation Date</b>	The date that the public distribution list was created.
<b>List Alias</b>	The short name of the public distribution list.
<b>Count</b>	The number of subscribers and other public distribution lists that are members of the public distribution list.
<b>Distribution List Name</b>	The name of the public distribution list.
<b>Owner First and Last Name</b>	The subscriber or public distribution list that owns the public distribution list.  If the List All Members check box is checked, this column also includes the names of subscribers and other public distribution lists that are members of the public distribution list.
<b>Member List</b>	This column is not used.

## Failed Login Report

The Failed Login report includes information about failed phone user logons as well as failed Cisco Unity Administrator logons. Use the Failed Login report to identify patterns of invalid logons, which would indicate that an individual is trying to gain unauthorized access to Cisco Unity. The report also identifies accounts that have been locked because the maximum number of invalid logons has been exceeded.

You can generate the Failed Login report for all subscriber accounts. Additionally, you can indicate whether to show all failed logon attempts (expand the report) or show only the last failure for each subscriber.

Note that including the Failed Login report for the Cisco Unity Administrator logons requires that auditing be enabled in system security policies. Cisco Unity setup enables auditing by default.

The Failed Login report includes the following information about failed phone user logons:

<b>Subscriber/User Name</b>	The display name of the subscriber whose account experienced the failed logon. Note that the select option to choose a subscriber is not supported for this release.
<b>Alias</b>	The short name of the subscriber whose account experienced the failed logon.
<b>Caller ID (Phone Number Called From)</b>	The calling number, if known, from which the logon was attempted.
<b>Subscriber DTMF</b>	The unique DTMF access code that callers dial to access this account.
<b>Date and Time</b>	The date and time of the failed logon.
<b>Maximum Failures Exceeded</b>	Whether the failed logon exceeded the maximum number allowed; if so, the account is locked.
<b>Failure Number</b>	A running total of failed logons by subscriber or by day, depending on how the report is sorted.
<b>Source</b>	Indicates either Standard when a subscriber uses normal Cisco Unity password security, or Enhanced when a subscriber uses enhanced phone security to log on.

The Failed Login report also includes the following information about failed Cisco Unity Administrator logons:

<b>User Name</b>	The logon name assigned to the subscriber.
<b>Computer</b>	The name of the workstation, if known, from which a subscriber attempted to log on.
<b>User Domain</b>	The Windows domain name assigned to a subscriber.
<b>Event ID</b>	The Windows event ID that was generated when the logon failed.
<b>Date and Time</b>	The date and time of the failed logon.
<b>Failure Number</b>	A running total of failed logons by subscriber or by day, depending on how the report is sorted.

## Transfer Billing Report

Use the Transfer Billing report to obtain information about calls that are transferred from a subscriber account or from a call handler. You can use this report for billing purposes or to keep track of transfers to long distance phone numbers. You can generate the report for all subscribers, or all billing IDs, or for a single distribution list or single call handler. Note that the single subscriber, single billing ID, distribution lists, and all call handler selection options are not supported in this release.

Only those subscribers with call transfer data appear on the report.

The Transfer Billing report includes the following information:

<b>Name</b>	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) from which the call was transferred.
<b>Extension</b>	The extension of the Cisco Unity entity (such as subscriber, call handler, or interview handler) from which the call was transferred.
<b>Billing ID</b>	The billing ID of the Cisco Unity subscriber from which the call was transferred.  If the Cisco Unity billing ID for a subscriber is blank (the Billing ID field on the Subscribers > Account screen), then 0 (zero) is listed as the value for this field on the report.  Note that other entities from which calls are transferred, such as call handlers, directory handlers, and interview handlers, do not have billing IDs.
<b>Date</b>	The date that the transfer occurred.
<b>Time</b>	The time that the transfer occurred.
<b>Dialed Number</b>	The number that the call was transferred to.
<b>Transfer Result</b>	The result of the call. Possible results include: <ul style="list-style-type: none"> <li>• Connected—The called party answered the phone.</li> <li>• Busy—The dialed number was busy.</li> <li>• RNA (Ring No Answer)—The dialed number did not answer.</li> <li>• Released—The result is unknown.</li> </ul>

## Outcall Billing Report

Use the Outcall Billing report to obtain information about outbound calls made by Cisco Unity for message notifications. This report also provides information about outbound calls that Cisco Unity makes to subscriber extensions when subscribers use their phones as the recording and playback device for the Media Master. You can use this report for billing purposes, or to keep track of message notifications sent to long distance phone numbers. You can generate the report for subscribers, billing IDs, or for a distribution list.

The Outcall Billing report includes the following information.

Note that the Dial Time option is not supported in this release.

<b>Name</b>	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) which made the call.
<b>Extension</b>	The extension of the Cisco Unity entity (such as subscriber, call handler, or interview handler) which made the call.
<b>Billing ID</b>	The billing ID of the Cisco Unity subscriber from which the call was transferred.  If the Cisco Unity billing ID for a subscriber is blank (the Billing ID field on the Subscribers > Account screen), then 0 (zero) is listed as the value for this field on the report.  Note that other entities from which calls are transferred, such as call handlers, directory handlers, and interview handlers, do not have billing IDs.

<b>Time</b>	The time that Cisco Unity made the call.
<b>Delivery Device</b>	The notification device that the message was sent to, which can be a home phone, work phone, spare phone, or pager. When the phone is used as the recording and playback device for the Media Master, the word “TRAP” (Telephone Record And Playback) is listed as the delivery device.
<b>Dialed Number</b>	The phone number of the delivery device.
<b>Result</b>	The result of the call. Possible results include: <ul style="list-style-type: none"> <li>• Busy—The dialed number was busy.</li> <li>• Connected—The called party answered the phone.</li> <li>• Failure—The call failed.</li> <li>• Port Disabled—All ports for outgoing calls have been disabled.</li> <li>• Port Unavailable—No ports were available for the outgoing call.</li> <li>• RNA (Ring No Answer)—The dialed number did not answer.</li> <li>• Release—The result is unknown. This typically happens for notifications sent to pagers.</li> <li>• Unknown—The result is unknown.</li> </ul>
<b>Call Time (Seconds)</b>	The length of the call, in seconds.

## Administrative Access Activity Report

Use the Administrative Access Activity report to track which system administrators changed values in Cisco Unity during a specified period and the changes they made. You can generate this report for all administrators. The option to select a single administrator is not supported in this release.

The Administrative Access Activity report includes the following information:

<b>Date and Time</b>	The date and time that the administrator created, deleted, or updated data for a Cisco Unity entity (such as subscriber, call handler, or interview handler).
<b>Administrator's Short Name</b>	The administrator short name.
<b>Administrator's First and Last Name</b>	The name of the administrator.
<b>DTMF ID</b>	The extension assigned to the administrator.
<b>Administrative Action</b>	Whether the administrator action created, updated, or deleted data for a Cisco Unity entity.
<b>Object</b>	The type of Cisco Unity entity (such as subscriber, call handler, or interview handler) that the administrator created, deleted, or updated.
<b>Name</b>	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) that the administrator created, deleted, or updated.
<b>Field (Property)</b>	The name of the field from the page in the Cisco Unity Administrator that was changed in creating, updating, or deleting data for a Cisco Unity entity.
<b>Value</b>	The new value for the changed field.

## Event Log Report

Use the Event Log report to list events from the Windows application log. You can generate the report for all application events on the Cisco Unity server, or for the events that apply only to Cisco Unity. Note that Cisco Unity writes events only to the Windows application log; it does not write events to the system or security logs. If you generate a report for all application events, you can identify the Cisco Unity events as those events that begin with “CiscoUnity” or “AV” (for example, “CiscoUnity\_LogMgr”).

You can also view application events by using the Windows Event Viewer (on the Windows Start menu, click Programs > Administrative Tools > Event Viewer). For more information on Windows events, refer to the Windows Event Viewer online Help.

The Event Log report includes the following information:

<b>Date and Time</b>	The date and time that the event occurred.
<b>Type</b>	The Windows event type.
<b>Source</b>	The component that caused and logged the event.
<b>Message (Msg) ID</b>	The event ID.
<b>Computer</b>	The server on which the event occurred.
<b>More Info</b>	A message that contains additional information about the event.

## Port Usage Report

You can use the Port Usage report to determine if the voice messaging system is running close to capacity, and indicate a specific port or ports to include in the report. Enter port numbers or ranges of numbers separated by commas (for example, 1,2,4-8) in the Ports to Show field. Note that this report fails if the specific port numbers or ranges that are entered are not valid (for example, do not enter a port range of 10–50 if there are only 48 ports on the system.)

As an alternative to the Port Usage report, we recommend using the Port Usage Analyzer, available in Tools Depot. For more information, see the Port Usage Analyzer online help.

The Port Usage report includes the following information:

<b>Port Number</b>	The Cisco Unity port number.
<b>Unit of Time</b>	The unit of time by which data is broken down for the time period that you specified in the Date Range. Depending on the length of the time period, data is broken down into hours, days, and weeks.
<b>Date Range</b>	The range of dates for which data is included.
<b>Time</b>	The specific hour or date(s) by which data is broken down for the time period that you specified in the Date Range.
<b>Ports</b>	The ports included in the report.
<b>Number of Calls</b>	The number of calls processed by the port per hour, day, or week for the time period specified.
<b>Length of Calls</b>	The total length, in milliseconds, of all calls on the port per hour, day, or week for the time period specified.

<b>Average Length of Calls</b>	The average length, in seconds, of all calls on the port per hour, day, or week for the time period specified.
<b>Percent Utilization</b>	The percentage of available time that a port was in use per hour, day, or week. Note that it is recommended that the value of Percent Utilization not exceed 80 percent of the ports used for incoming calls during peak usage.
<b>Average Calls Per Hour</b>	The average number of calls per hour for each port.
<b>Average Calls Per Day</b>	The average number of calls per day for each port. This information is provided only on the row that contains the summary for the week.

## System Configuration Report

Use the System Configuration report to get information about the Cisco Unity server and software. You also can view this information in the Cisco Unity Administrator on the Configuration pages.

The System Configuration report includes the following information:

<b>Serial Number</b>	This field is not applicable to the current version of the report.
<b>OEM Code</b>	This field is not applicable to the current version of the report.
<b>Product</b>	The name of the software product and version number.
<b>Number of Voice Ports</b>	The number of voice ports licensed for the Cisco Unity system.
<b>Languages</b>	The number of language licenses.
<b>Available Licenses and Total Licenses</b>	The available and total number of Cisco Unity licensed features, such as Digital Networking.
<b>Leading Silence for Recordings</b>	The length of silence, in seconds, allowed at the beginning of a recording. When the leading silence is longer than specified, Cisco Unity stops recording and discards the recording.
<b>Trailing Silence for Short and Long Recordings</b>	The length of silence, in seconds, allowed at the end of recordings that are 30 seconds or less and of recordings that are more than 30 seconds. When the trailing-silence limit is reached, Cisco Unity assumes the recording is finished and stops recording.
<b>Minimum Length for a Recording</b>	The minimum length of a recording, in seconds. When a recording is shorter than the minimum length, it is discarded.
<b>Computer and Windows Domain Name</b>	The Cisco Unity server name on the network and the Windows domain name.
<b>Total Hard Drive Space, Total Used Hard Drive Space, and Total Free Space</b>	The total size of all hard disks, the total amount of space in use, and the total free space on the Cisco Unity server.
<b>Additional Settings</b>	The report contains additional information about the Cisco Unity server and software, such as integration type, Cisco Unity Assistant licensing, and the Text to Speech engine.  (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

## Unresolved References Report

Use the Unresolved References report to locate primary call handlers (those call handlers that are associated with a subscriber account), other call handlers, and interview handlers that are left unresolved because of the improper deletion of a subscriber account. The problem occurs when a subscriber is deleted by using Lotus Domino or Windows administrator applications without first deleting the subscriber by using the Cisco Unity Administrator.

If the report finds a problem with a call handler, directory handler, or interview handler, run the Cisco Unity DbWalker utility, available in Tools Depot, to repair the problem.

The Unresolved References report includes the following information:

<b>Handler Name</b>	The name of the unresolved handler.
<b>Handler/Access ID</b>	The extension (if any) associated with the handler.
<b>Handler Type</b>	The type of handler found to be in an unresolved state. The type can include call handlers, interview handlers, the directory handler, or primary call handlers.
<b>Owner</b>	The owner of the handler.
<b>Message Recipient</b>	The message recipient associated with the handler.

## Call Handler Traffic Report

Use the Call Handler Traffic report to track the number of calls routed by call handlers, and how callers chose to exit the handlers.

This report can only be run for all call handlers. Note that the option to select a single call handler is not supported in this release.

There are four ways a caller can exit a call handler: by hanging up, by choosing a one-key dialing option, by dialing an extension that transfers the call to another call handler (or subscriber), or by being routed automatically by the after-greeting action specified in the call handler.

The Call Handler Traffic report includes the following information:

<b>Start Time</b>	The specific hour or date(s) by which data is broken down for the time period that you specified in the Date Range.
<b>Total Calls</b>	The total number of calls routed to the call handler.
<b>Method Callers Use to Exit a Call Handler</b>	The total number of times each exit method is used by callers. Callers can exit a call handler by hanging up, pressing a one-key dialing option, dialing an extension that transfers the call to another call handler (or subscriber), or by being routed to another call handler (such as the Goodbye call handler) as specified by the after-greeting action.
<b>Key</b>	The number of calls in which the caller exited the call handler by pressing a one-key dialing option. The report includes a tally for each key.
<b>DTMF ID</b>	The number of calls in which the caller exited the call handler by dialing a valid extension to transfer to another call handler (or subscriber).
<b>Invalid DTMF ID</b>	The number of calls routed to the default Error call handler because the caller dialed an invalid extension.

<b>After Greeting Action</b>	The number of calls routed according to the after greeting action specified for the call handler.
<b>Hang-Up</b>	The number of calls in which the caller exited the call handler by hanging up.



## Network Settings

---

### Overview: Network Settings

You use the network settings to set up and administer Cisco Unity for networking with other Cisco Unity servers. The term networking has a broad definition and encompasses the following ideas:

- Subscribers associated with one Cisco Unity server can use the phone to send voice messages to:
  - Subscribers associated with another Cisco Unity server.
  - Individuals with access to a computer connected to the Internet.
- Unidentified callers can find any subscriber in the phone directory and leave a voice message. Depending on the phone system and network configuration, unidentified callers who reach the Cisco Unity automated attendant or directory assistance can be transferred to any subscriber phone, even to the phone of a subscriber who is not associated with the local server.

Cisco Unity provides the following networking options:

- **Digital Networking**—Allows messaging among multiple Cisco Unity servers connected to a single, global directory. The message transport agent (MTA) is the message transport mechanism between servers. You use this option when the Cisco Unity servers access a shared voice mail directory.
- **Internet Subscribers**—Allows messaging between Cisco Unity subscribers and individuals with access to a computer connected to the Internet.

No matter which networking option you use, you always customize the primary location settings for your Cisco Unity server.

See the following sections in this chapter for more information about network settings:

- [Primary Location Profile Settings, page 27-2](#)
- [Primary Location Addressing Option Settings, page 27-3](#)
- [Delivery Location Profile Settings, page 27-5](#)
- [Monitored Domain Address Books, page 27-5](#)

For more information about networking, refer to the *Networking in Cisco Unity Guide*, available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/net/net403/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/net/net403/dom/index.htm).

## Primary Location Profile Settings

Each Cisco Unity server has a primary location, which is created during installation and which cannot be deleted. The primary location identifies the Cisco Unity server and contains the networking information needed to communicate with other Cisco Unity servers. With the exception of public distribution lists, all subscribers and other Cisco Unity objects (such as call handlers) created on your Cisco Unity server are associated with the primary location.

No matter which networking option Cisco Unity uses to send and receive voice messages, you need to customize the primary location of your Cisco Unity server.

Use the following table to learn more about the profile settings for the primary location.

**Table 27-1 Network > Primary Locations > Profile Page**

Field	Considerations
Display Name	This displays the name of the primary location. To change the name, enter a new name here, and then click the Save icon.
Dial ID	<p>Enter the ID that identifies the primary location. Enter numbers only, up to a maximum of 10 digits. The default minimum length is 3 digits.</p> <p>Although the minimum length for Dial IDs can be reduced by using the Advanced Settings Tool, one- and two-digit Dial IDs may conflict with private distribution list IDs during an address search. When a subscriber addresses a message by entering a one- or two-digit number, Cisco Unity first searches for a matching private distribution list. If a match is found, the search stops. Therefore, when a subscriber addresses a message by entering a location Dial ID to narrow down the search scope to a particular location, if the number entered matches a private distribution list ID, the conversation offers only the private distribution list as a destination. If subscribers do not address messages to other locations by first entering a Dial ID, there is no conflict and the minimum length for Dial IDs can be reduced to accommodate complex dial plans.</p> <p>The following policies are recommended:</p> <ul style="list-style-type: none"> <li>• Establish a fixed length for Dial IDs and if possible, a fixed length for extensions.</li> <li>• Assign unique Dial IDs.</li> <li>• If you use variable-length Dial IDs and extensions, the Dial IDs should be in a different numbering range than extensions.</li> <li>• If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs. (For example, do not create Dial IDs like 432 and 4325.)</li> </ul>

Table 27-1 Network &gt; Primary Locations &gt; Profile Page (continued)

Field	Considerations
Recorded Name	<p>Record a name for the primary location. The conversation plays the recorded name for this primary location when:</p> <ul style="list-style-type: none"> <li>Subscribers associated with a Cisco Unity server in a different dialing domain address a message to subscribers associated with this location. (For example, assuming that New York is the recorded name for this location: “There are two matches. For John Smith, at New York, press 1. For Mary Smith press 2.”)</li> <li>Subscribers associated with a Cisco Unity server in a different dialing domain listen to messages from subscribers associated with this location. (For example: “Message 1, a voice message, from John Smith at New York....”)</li> <li>The setting Include Locations in Searches on the Network &gt; Primary Location &gt; Addressing Options page is enabled on another primary location. When subscribers at the other location address a message, the recorded name for this primary location may be played in the message addressing search results along with subscriber names. (For example: “There are two matches. For Chris Newton, press 1. For New York, press 2.”)</li> </ul> <p>To record the name here, use the Media Master control bar. (Note that the Media Master is not available across a firewall.) Use the Options menu in the Media Master control bar to set recording and playback devices, if applicable, and to use other sound files.</p>
Dialing Domain	<p>Select from the list or enter the name of the dialing domain of which this location is a member. A dialing domain is a collection of Cisco Unity servers that are integrated with the same phone system or phone system network. Extensions within a dialing domain must be unique. The dialing domain allows Cisco Unity to handle overlapping extensions on Cisco Unity servers that are outside of the dialing domain.</p> <p>A dialing domain provides a means to scope message address and directory handler searches so that Cisco Unity does not search the entire global directory.</p> <p>The default setting is None. Use the default when:</p> <ul style="list-style-type: none"> <li>Your installation consists of only one Cisco Unity server.</li> <li>Your installation consists of two or more Cisco Unity servers, but each server is integrated with a separate phone system.</li> </ul> <p>There is no limit to the number of Cisco Unity servers that can be assigned to a single dialing domain, and there is no limit to the number of dialing domains. However, a Cisco Unity server can be a member of only one dialing domain.</p>

## Primary Location Addressing Option Settings

The primary location addressing options allow you to control the scope of the search that Cisco Unity performs when searching for a matching extension in the following cases:

- When a subscriber addresses a message by using the phone.
- When subscribers add members to private lists by using the phone or the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)
- When an administrator adds members to public or private distribution lists by using the Cisco Unity Administrator.

You can set the scope to the local Cisco Unity server, to the dialing domain that the local Cisco Unity server is a member of, or to the entire global directory.

Use the following table to learn more about location addressing option settings.

**Table 27-2 Network > Locations > Addressing Options Page**

Field	Considerations
Subscriber Searches: Limit Searches To	<p>Select the scope of the search that Cisco Unity performs when a subscriber addresses a message by using the phone, and when members are being added to a public or private distribution list:</p> <ul style="list-style-type: none"> <li>• Local Server—Limits the search to subscribers created on the local Cisco Unity server.</li> <li>• Dialing Domain—If a match is not found while searching the local Cisco Unity server, the search expands to include subscribers created on other Cisco Unity servers that are in the same dialing domain as the local Cisco Unity server.</li> <li>• Global Directory—After searching the local Cisco Unity server and then the dialing domain (if there is one), the search expands to include every subscriber created on other Cisco Unity servers in the directory.</li> </ul>
Include Locations in Searches	<p>Check this check box to have locations included in searches. For this setting to be useful to subscribers, locations need to have recorded voice names.</p> <p>When checked, this setting allows subscribers to address a message in two steps. First subscribers select a particular location (either by spelling the name or by entering the Dial ID). If Cisco Unity finds a matching location, the recorded voice name for the location is played (assuming one has been recorded), and subscribers are prompted to either by spell the name or enter the extension of the recipient. This allows subscribers to limit a search for a recipient to a specific location.</p> <p>This option is useful when the global directory is large and addressing a message by name results in many matches.</p> <p>For example, assume there are two Cisco Unity servers that use Digital Networking to exchange messages. Assume 100 is the Dial ID for the primary location of the remote Cisco Unity server, and that a voice name for the location has been recorded.</p> <ul style="list-style-type: none"> <li>• A subscriber enters 100# to address a message to someone on the other Cisco Unity server.</li> <li>• When the primary location 100 is found, the conversation plays, “For location &lt;Recorded voice name&gt;, press #.”</li> <li>• When the sender presses # to confirm, the conversation plays, “Enter the extension followed by #.”</li> <li>• The subscriber enters 12345#. If Cisco Unity finds a matching subscriber extension at location 100, the conversation plays, “For &lt;Subscriber recorded voice name&gt; at extension 12345, press #.”</li> <li>• When the sender presses # to confirm, the conversation plays, “Added. To add another name, press 1. To record the message, press #.”</li> </ul>

## Delivery Location Profile Settings

When more than one Cisco Unity server is networked together via Digital Networking, information about the primary locations on other Cisco Unity servers is displayed on the Delivery Location page. This information is display only.

Use the following table to learn more about the profile settings for delivery locations.

**Table 27-3** *Display Only Information About Primary Locations on Other Cisco Unity Servers*

Field	Consideration
Name	Displays the name of a primary location.
Dial ID	Displays the Dial ID of a primary location.
Recorded Name	The recorded name of the primary location.
Destination Type	Although SMTP is displayed as the Destination Type, messaging between Cisco Unity servers in the same directory is not done by SMTP.
Domain Name	The domain name of the primary location.

## Monitored Domain Address Books

The Domino address book(s) displayed on the Monitored Address Books page are the ones specified on System > Configuration > Subscriber Address Books page. These address book(s) contain the user information that allows messaging with subscribers on another Cisco Unity server via Digital Networking. Each Cisco Unity server monitors these address books for data from other Cisco Unity servers. Information about locations and subscribers created on other Cisco Unity servers is stored in each server's SQL database (called UnityDb) in the GlobalLocation and GlobalSubscriber tables.

**Table 27-4** *Network > Digital Networking Options > Monitored Address Books Page*

Field	Considerations
Domain	The domain in which the monitored address book resides.
Server	The Domino server that the address book is located on.
Address Book	The address book that contains the user information that allows messaging with subscribers on another Cisco Unity server. For Digital Networking to work, all the Cisco Unity servers in the network need to monitor the primary address book in the domain names.nsf.
Display Name	The display name for the address book. This name allows you to more easily distinguish the address book from other address books Cisco Unity may use. Note that the Display Name field does not correspond to any fields in the Domino Administrator.





## System Settings

### Overview: System Settings

Before Cisco Unity can be set up to handle calls and messages, some basic system settings must be entered.

See the following sections in this chapter for more information:

- [Configuration Settings, page 28-2](#)—This section provides information about the configuration settings.
- [Software Versions, page 28-4](#)—This section details where to find version numbers for Cisco Unity and other software components.
- [Recording Settings, page 28-4](#)—This section provides information about recording settings.
- [Contacts, page 28-5](#)—This section details where you can enter the names and phone numbers of the people responsible for maintaining or administering the Cisco Unity server.
- [Phone Languages Settings, page 28-5](#)—This section provides information about the language played for subscribers and unidentified callers.
- [GUI Languages Settings, page 28-6](#)—This section provides information about the language in which the Cisco Unity Administrator and Cisco Personal Communications Assistant are displayed.
- [Subscriber Address Book Settings, page 28-7](#)—This section provides information about how Domino address books are used to create Cisco Unity subscriber accounts.
- [Schedule Settings, page 28-9](#)—This section explains how to set up system schedules.
- [Holiday Settings, page 28-10](#)—This section explains how to set up holidays to work with Cisco Unity schedules.
- [Licensing Status, page 28-11](#)—This section provides information about user and feature licenses.
- [Authentication Settings, page 28-11](#)—This section provides information about logon, password, and account lockout policy settings for subscribers accessing Cisco Unity web clients.
- [Voice Messaging Port Settings, page 28-14](#)—This section provides information about setting up voice ports.
- [Cisco CallManager Integration, page 28-15](#)—This section provides information on the Cisco CallManager integration settings that are displayed.
- [SIP Integration, page 28-16](#)—This section provides information on the SIP integration settings that are displayed.
- [Circuit-Switched Integration, page 28-17](#)—This section provides information on the circuit-switched integration settings that are displayed.

- [Setting a Warning Tone for End of Recording, page 28-19](#)—This section describes how to enable a warning tone to play before the maximum allowable message length of a recording is reached.
- [Remapping Extension Numbers, page 28-20](#)—This section describes how to remap the calling numbers and forwarding numbers of calls that Cisco Unity handles to the extensions of your choice.

## Configuration Settings

Configuration settings contain general Cisco Unity settings such as the default schedule, system security, and the cleanup interval for log files, as well as information about the Cisco Unity server.

Use [Table 28-1](#) to learn more about configuration settings. See the following for additional information on these related topics:

- Setting up enhanced phone security—See the [“Overview: Enhanced Phone Security” section on page 10-1](#).
- Identifying the default system schedule—See the [“Schedule Settings” section on page 28-9](#).

**Table 28-1 System > Configuration > Settings Page**

Field	Considerations
Default Schedule	Select the default schedule, which is used for all Cisco Unity operations unless specifically changed for a call handler, subscriber account, or call routing table.  Default: Weekdays.
Use 24-Hour Time Format for Conversation and Schedules conversation	Check this check box to use a 24-hour time format for all Cisco Unity operations. For example, 1:00 P.M. is shown as 13:00 in the Cisco Unity Administrator, and subscribers hear 13:00 when listening to the timestamps for their messages over the phone.  When this check box is left unchecked, Cisco Unity uses the 12-hour clock format as the system default.
Enable Spelled Name Search	Check this check box to allow subscribers to address messages to other subscribers by spelling the subscriber first or last name over the phone. In addition, when this check box is checked, subscribers who are editing private lists can search for subscribers by spelling the subscriber name over the phone. Addressing by name requires lettered keypads on subscriber phones.  Note that checking this check box does not prevent subscribers from searching for subscribers by entering subscriber extensions over the phone when editing private lists or addressing messages. In the subscriber conversation, subscribers can switch between addressing by name and addressing by extension by pressing the # key twice.  When this check box is unchecked, subscribers can search for subscribers over the phone only by entering subscriber extensions. In addition, the option to address by spelled name cannot be used on the Subscribers > Conversation page and in the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)  Default: Check box checked.

Table 28-1 System &gt; Configuration &gt; Settings Page (continued)

Field	Considerations
RSA Two Factor	<p>Check this check box to enable enhanced phone security, which uses RSA two-factor user authentication. To use enhanced phone security, an ACE/Server must be installed and configured for your system. Additionally, you must create a new class of service (COS) or modify an existing COS for the subscribers who are using enhanced phone security.</p> <p>To disable enhanced phone security, uncheck this check box, and then change every affected COS to use regular phone security. Otherwise, subscribers who are members of an enhanced phone security COS will not be allowed to log on to Cisco Unity.</p> <p>Default: Check box not checked.</p>
Subscribers Are Identified as Message Senders Only if They Log On	<p>Check this check box to disable identified subscriber messaging system-wide.</p> <p>When identified subscriber messaging is enabled, Cisco Unity automatically identifies a message left during an internal call as originating from the extension from which the call was made.</p> <p>When identified subscriber messaging is disabled, Cisco Unity does not identify the originating extension of a message left during an internal call, unless the calling subscriber logs on to Cisco Unity before leaving the message.</p> <p>Regardless of enabled or disabled status, if a subscriber logs on before leaving a message from an internal location other than the extension assigned to the subscriber (such as from a conference room), Cisco Unity identifies the call as originating from the extension of the logged-on subscriber, rather than the extension from which the call is placed.</p> <p>This field is applicable only when the phone system provides caller and called party information to Cisco Unity. It is a system-wide setting that is not configurable for an individual subscriber or subscriber template.</p> <p>Default: Check box not checked.</p>
Cleanup Interval for Logger Data Files in Days	<p>Indicate how often data files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files.</p> <p>Default: Seven days.</p>
Cleanup Interval for Logger Diagnostic Files in Days	<p>Indicate how often diagnostic files should be deleted. Cisco Unity waits the specified number of days before automatically deleting the files.</p> <p>Default: Seven days.</p>
Replicate Cisco Unity Directory Objects	<p>Choose Changed Objects to manually synchronize changes from the IBM Lotus Notes Directory into the Cisco Unity SQL database. For example, changing the distribution list by which the directory handler is scoped requires a synchronization. This synchronization takes place automatically when the Cisco Unity directory services (AvDSAD and AvDSGlobalCatalog) poll the directory for any changes to be applied to the SQL database, which usually occurs within 15 to 20 minutes after the directory handler scope change is made in the Cisco Unity Administrator, or can be done immediately by choosing Changed Objects.</p> <p>Choose All Objects only if Cisco Unity has been down for a considerable length of time.</p>
Cisco Unity Computer Settings	<i>Display only.</i> This setting shows the name of the Cisco Unity server and the Windows Domain name.
Fax Settings	This setting shows the name of the fax domain.
Disk Usage	<i>Display only.</i> This setting shows, in megabytes, the total, used, and free disk space on the Cisco Unity server.

## Software Versions

The System > Configuration > Software Versions page displays the Cisco Unity serial and build numbers, and the version numbers for several Cisco Unity components and for the Microsoft Windows 2000 Server. If you ever contact the Cisco Technical Assistance Center (TAC), you may need to refer to this information.

## Recording Settings

The Recordings page contains settings for recording time limits and for silence thresholds (the amount of silence before Cisco Unity assumes the caller is no longer on the line) before, during, and after recordings.

## Audio Codecs

Cisco Unity supports the following audio codecs:

Audio Codec	Approximate File Size, 1-Minute Message	Quality Rating
G.711 Mu-Law and A-Law	480 KB	Excellent
Dialogic OKI ADPCM 8Khz	240 KB	Fine
Dialogic OKI ADPCM 6Khz	180 KB	Fine
GSM 6.10	98 KB	Fine
G.729a	60 KB	Good



### Note

GSM 6.10 is supported for playback on a Pocket PC, and is a higher quality recording format than MP3.

For information on choosing and implementing audio codecs, refer to the *White Paper: Audio Codecs and Cisco Unity*, which is available at

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/whitpaper/codecs.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpaper/codecs.htm).

Use the following table to learn more about recording settings.

**Table 28-2 System > Configuration > Recordings Page**

Field	Considerations
Allowed Time for Recording in Milliseconds	Select the number of milliseconds for the DTMF clip length. This setting indicates how much to truncate the end of a recording when a message is terminated with a touchtone.  Default: 170 milliseconds.
Allowed Time for Short Recording in Seconds	Select the number of seconds that Cisco Unity uses as a cutoff for short and long recordings. Recordings shorter than this number are considered to be a short recording; recordings longer than this number are considered to be a long recording.  Default: Ten seconds.

**Table 28-2 System > Configuration > Recordings Page (continued)**

Field	Considerations
Allow How Much Silence Before Time Out in Seconds	Select the number of seconds after which Cisco Unity will end the message, greeting, or recorded name if the subscriber or caller has not begun speaking. A value lower than two or three seconds may not give the subscriber or caller enough time to begin speaking. Default: Five seconds.
Discard Any Recording Less Than in Seconds	Select the minimum length of recordings, in seconds, for messages or greetings. Note that this setting is not applied to recorded names. Default: One second.
Short Recording (Short Recording Trail Limit or Less)	Select the number of seconds of silence that Cisco Unity uses to detect the end of a short recording. When Cisco Unity detects a pause equal to the number of seconds specified, Cisco Unity assumes that the speaker has finished recording the message, greeting, or recorded name. Callers are more likely to pause longer during long messages, so you may want to set a smaller pause length for short recordings than for long recordings. Cisco Unity uses the Allowed Time for Short Recording in Seconds setting to determine whether a recording is short or long. Default: Two seconds.
Long Recording (Over Short Recording Trail Limit)	Select the number of seconds of silence that Cisco Unity uses to detect the end of a long recording. When Cisco Unity detects a pause equal to the number of seconds specified, Cisco Unity assumes that the speaker has finished recording the message, greeting, or recorded name. Callers are more likely to pause longer during long messages, so you may want to set a greater pause length for long recordings than for short recordings. Cisco Unity uses the Allowed Time for Short Recording in Seconds setting to determine whether a recording is short or long. Default: Three seconds.

## Contacts

The System > Configuration > Contacts page is where you enter the names and phone numbers of the people responsible for maintaining or administering the Cisco Unity server. This information might be useful to a technician who is accessing Cisco Unity from off-site.

## Phone Languages Settings

Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers. You specify a default phone language and other system-wide phone language settings, as well as the default Text to Speech (TTS) language, which is the language that subscribers hear when their e-mail is read to them over the phone. Note that to use TTS languages, your organization must have TTS e-mail and the applicable languages installed. See the [“Setting Up Languages” section on page 11-1](#) for more information about using multiple languages.

If desired, you can customize the language settings for specific Cisco Unity components such as subscriber accounts, routing rules, call handlers, interview handlers, and directory handlers. See the [“Specifying Phone Languages” section on page 11-3](#) for information about customizing language settings for individual Cisco Unity components.

Use the following table to learn more about phone languages settings.

**Table 28-3 System > Configuration > Phone Languages Page**

Field	Considerations
License Counts – Total	<i>Display only.</i> This setting shows the total number of phone language licenses for your installation, which determines how many phone languages can be loaded at one time. Note that the number of phone language licenses does not limit the number of phone languages actually installed on the Cisco Unity server.
License Counts – Loaded	<i>Display only.</i> This setting shows the number of languages in the Loaded list.
License Counts – Unused	<i>Display only.</i> This setting shows the number of unused phone language licenses. Note that this number might not be the same as the number of languages in the Available list.
Available	This list displays the languages that have been installed on the Cisco Unity server but that are not currently loaded.  When you load a language by moving it from the Available list to the Loaded list, the Loaded and Unused License Count fields are adjusted accordingly. You can move languages to the Loaded list only if the Unused License Count is greater than zero.
Loaded	This list displays the languages that can be selected for use by the subscriber conversation and various Cisco Unity components such as call handlers.  When you unload a language by moving it from the Loaded list to the Available list, the Loaded and Unused License Count fields are adjusted accordingly. Any call handlers or other Cisco Unity components that were using the unloaded language will now be reset to use the default phone language.
Default Phone Language	Select the default language in which system prompts are played to subscribers and callers. Only the languages shown in the Loaded list can be chosen as the default language.
Default Text to Speech Language	Select the default language that subscribers hear when having their e-mail read to them over the phone. This is typically the same language that you selected in the Default Phone Language field with the following exceptions: <ul style="list-style-type: none"> <li>• If you selected Australian or New Zealand English as your phone language, select either United States English or UK English as your default Text to Speech language.</li> <li>• There is no applicable Text to Speech language available for Brazilian Portuguese, Czech, or Korean.</li> </ul>

## GUI Languages Settings

The settings on the GUI Languages page determine the languages in which the Cisco Unity Administrator pages can be displayed. You specify a default GUI language and other system-wide GUI language settings.

To change the GUI language used in the Cisco Unity Administrator or the Cisco Personal Communications Assistant, select a language in the browser. (Subscribers use the Cisco PCA website to access the Cisco Unity Assistant. Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

For the Cisco Unity Administrator, note that the language selected in the browser must be one of the languages in the Loaded list on the GUI Languages page. If the language that you select in the browser is not among the loaded languages, Cisco Unity uses the default GUI language. For the Cisco PCA, the language selected in the browser must be one of the languages that the Cisco PCA offers.

Use the following table to learn more about GUI languages settings.

**Table 28-4** System > Configuration > GUI Languages Page

Field	Considerations
License Counts – Total	<i>Display only.</i> This setting shows the total number of GUI language licenses for your installation, which determines how many GUI languages can be loaded at one time. Note that the number of GUI language licenses does not limit the number of GUI languages actually installed on the Cisco Unity server.
License Counts – Loaded	<i>Display only.</i> This setting shows the number of languages in the Loaded list.
License Counts – Unused	<i>Display only.</i> This setting shows the number of unused GUI language licenses. Note that this number might not be the same as the number of languages in the Available list.
Available	This displays the languages that have been installed on the Cisco Unity server but that are not currently loaded.  When you move a language from the Available list to the Loaded list, the Loaded and Unused License Count fields are adjusted accordingly. You can move languages to the Loaded list only if the Unused License Count is greater than zero.
Loaded	This displays the languages that can be used in the browser display of the Cisco Unity Administrator.  When you unload a language by moving it from the Loaded list to the Available list, the Loaded and Unused License Count fields are adjusted accordingly.
Default GUI Language	Select the default GUI language from the Loaded list. Cisco Unity uses the default GUI language only if the language selected in the browser is not among the loaded GUI languages.

## Subscriber Address Book Settings

By default, the Domino address book displayed on the System > Configuration > Subscriber Address Books page is the one that was specified during Cisco Unity installation. An address book contains user data that you can import into Cisco Unity when you create new subscriber accounts by using the Cisco Unity Administrator. To authenticate subscribers who access the Cisco Personal Communications Assistant (PCA), Cisco Unity searches the Domino Address Book for a Person document associated with the user name that the subscriber entered on the Cisco Unity Log On page. This is also true when the Cisco Unity Administrator uses the Anonymous authentication method and the subscriber enters Domino credentials on the Cisco Unity Log On page.

You can use the following procedure to add additional address books to this page, but it is not recommended that you add more than one. You should consider bandwidth issues if you add an address book for a Domino server that resides in another domain. Finally, note that you must restart the Cisco Unity server before any changes that you make to this page can take effect.

### To Add an Address Book and Reconfigure Cisco Unity to Use It

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Subscriber Address Books** page.
  - Step 2** Click **Add**.
  - Step 3** Enter the Server, Address Book, and Display Name information in the applicable fields.

- Step 4** Click the **Save** icon.
- Step 5** Follow the system prompts. (You will be asked to restart the Cisco Unity server and run the Cisco Unity SysCheck tool.)
- Step 6** When Cisco Unity has restarted, do the [“To Check the Cisco Unity Configuration After Adding an Address Book”](#) procedure to confirm that the changes did not adversely affect the Cisco Unity configuration.

---

#### To Check the Cisco Unity Configuration After Adding an Address Book

---

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **SysCheck**.
- Step 3** On the Welcome to the Check Unity Configuration Wizard page, click **Select Configuration Tests**, and click **Next**.
- Step 4** Uncheck all check boxes, except the **Domino** check box.
- Step 5** Click **Test**.
- Step 6** In the Test Results box, click the link provided to view the test results.
- Step 7** If no errors are reported, proceed to [Step 8](#). Otherwise, do the following steps:
- Follow the advice offered in the Resolution column to correct each configuration or permissions error.
  - Return to the Completing the Check Unity Configuration Wizard page, and click **Finish**.
  - Repeat [Step 2](#) through [Step 7](#) until no errors are reported.
- Step 8** Click **Finish**.
- 

Use the following table to learn more about address book settings.

**Table 28-5 System > Configuration > Subscriber Address Books Page**

Field	Considerations
Domain	This is the domain in which the Domino server resides.
Server	The Domino server associated with the address book.
Address Book	This is the address book that contains the user data that you import when you create Cisco Unity subscriber accounts by using the Cisco Unity Administrator. Cisco Unity also uses the address book to authenticate subscribers who try to access the Cisco PCA, and subscribers who try to access the Cisco Unity Administrator or the Status Monitor when the Cisco Unity Administrator and Status Monitor use the Anonymous authentication method.
Display Name	The name that was specified for the address book during Cisco Unity installation.  If you are adding a new address book, enter a meaningful name here so that you can easily distinguish the address book from the other address books that you may be using with Cisco Unity. The display name that you enter here is displayed in the Address Book list on the Import a Domino Person page.  Note that the Display Name field does not correspond to any fields in the Domino Administrator.

# Schedule Settings

Schedules are one of the variables that Cisco Unity uses to manage calls. The standard and closed subscriber and call handler greetings play according to the days and times that you specify in a schedule.

Cisco Unity offers two predefined schedules: All Hours – All Days, and Weekdays, both of which can be modified. In addition, you can create up to 64 schedules for your organization to accommodate the standard working hours of different groups of employees. You can use either of the predefined schedules, or a new schedule that you create, as the default schedule for Cisco Unity. The default schedule is used for all call handlers, subscriber templates, and call routing tables, unless you specify a different schedule for each call handler, subscriber account, or call routing table to follow.

For each schedule that you create or modify, you identify the hours and days that make up the standard and closed hours, and whether the schedule changes for holidays:

<b>Standard hours</b>	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.)
<b>Closed hours</b>	The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.
<b>Holidays</b>	The time range defined on the System > Holidays page when the organization is closed. See the <a href="#">“Holiday Settings” section on page 28-10</a> for information about identifying holidays.

## To Create a New Schedule

- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page.
- Step 2** Click the **Add** icon.
- Step 3** In the Add a Schedule dialog box, enter information as applicable in the Name field.
- Step 4** Select **New Schedule** or **Based on Existing Schedule**. If you select Based on Existing Schedule, select the applicable schedule in the Based On field.
- Step 5** Click the **Add** button.
- Step 6** Check the **Observe Holidays** check box, if applicable.
- Step 7** Click boxes on the schedule grid until all open (standard) half hours are white and all closed half hours are gray. Note that you can use the Copy Day's Schedule field and >> functions to avoid clicking the same blocks for more than one day.
- Step 8** Click the **Save** icon.
- Step 9** To use this new schedule as the Cisco Unity default schedule, do the following [“To Specify the Default Schedule”](#) procedure.

### To Specify the Default Schedule

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page, and click **Change Default Schedule** from any schedule page.
- Note that when you click the link, you leave the schedule page, and move to the System > Configuration > Settings page.
- Step 2** In the Default Schedule field, click the schedule you want to use as the default for new call handlers, subscriber templates, and call routing tables.
- Step 3** Check the **Use 24-Hour Time Format for Conversation and Schedules** check box to use a 24-hour time format for all schedules, if desired.
- Step 4** Click the **Save** icon.
- 

### To Modify an Existing Schedule

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Schedules** page.
- Step 2** Click the **Find** icon.
- Step 3** Double-click the schedule that you want to modify.
- Step 4** Change settings as applicable, and then click the **Save** icon.
- Step 5** To use this new schedule as the system default schedule, do the [“To Specify the Default Schedule”](#) procedure.
- 

Use the following table to learn more about schedule settings.

**Table 28-6** System > Schedules Page

Field	Considerations
Observe Holidays	Check this check box to have Cisco Unity play closed (off-hour) greetings and to observe closed transfer rules on the dates defined on the System > Holidays page.
Click Individual Blocks to Set Hours	Click the blocks in the grid to change from closed to open (standard) hours. Click a block again to undo your change. Note that you can set open (standard) and closed hours for one day, then use the Copy Day's Schedule box to copy the settings to other days.
Copy Day's Schedule	Select a day to copy from the list, then select which days to copy the schedule settings to. Use the Copy Day's Schedule field and >> functions to avoid clicking the same blocks for more than one day.

## Holiday Settings

When a Holiday setting is in effect, Cisco Unity plays closed greetings and observes closed transfer rules. You can set up several years of holidays at a time, and you can copy the holidays from one year to the next, adjusting dates as necessary. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

### To Identify Days as Holidays

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Holidays** page.
  - Step 2** Click the **Add** icon.
  - Step 3** In the Add a Holiday dialog box, select the month, day, and year of the holiday.
  - Step 4** Click the **Add** button.
- 

### To Modify a Holiday

- 
- Step 1** In the Cisco Unity Administrator, go to the **System > Holidays** page.
  - Step 2** Click the date of the holiday listed for the applicable year.
  - Step 3** In the Edit Holiday For field, change settings as applicable, and then click the **Save** icon.
- 

Use the following table to learn more about holiday settings.

**Table 28-7 System > Holidays Page**

Field	Considerations
Edit Holiday For	Enter the applicable year, month, and day for the holiday that you want to modify.

## Licensing Status

When your organization purchased Cisco Unity, licenses were assigned according to the number of users and the number of voice messaging ports. In addition, your organization may have purchased licenses for optional features. You can view the number of licenses purchased, and the number that are used and unused, from the System > Licensing page. If you need additional licenses, contact your reseller.

## Authentication Settings

Authentication settings dictate the logon and lockout policy which applies when subscribers access Cisco Unity by using the Cisco Personal Communications Assistant (PCA). If the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, the policy that you specify on the System > Configuration > Authentication Provider page also applies when subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity. In addition, by using the applicable Authentication Provides pages, you can specify two logon and lockout policies for the Cisco Unity Administrator and the Status Monitor when they use Anonymous authentication: one that applies when subscribers use their Windows domain credentials to log on, and yet another that applies when subscribers use their Domino credentials to log on.

**Note**

Subscribers cannot use Windows credentials to log on to the Cisco PCA, even though the Cisco Unity Administrator appears to allow you to set up logon, password, and lockout policies for this purpose. The Cisco PCA fields on the System > Configuration > Authentication Provider for Windows page are not functional in the 4.0x version of Cisco Unity.

It is important to consider that when subscribers log on to the Cisco PCA, their credentials are sent across the network to Cisco Unity in clear text. The same is true if the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method. For increased security, it is therefore recommended that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol (see the [“Manually Setting Up Cisco Unity to Use SSL”](#) section on page 5-1 for details). As best practice, it is also recommended that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator and the Status Monitor, as they do to log on to the Cisco PCA.

Changes to authentication settings affect all Cisco Unity subscribers. You cannot change authentication settings for individual subscriber accounts, though you can lockout individual subscriber accounts to prevent subscribers from using the Cisco PCA, Cisco Unity Administrator, or Status Monitor to access Cisco Unity. (For details, see the [“Subscriber Account Settings”](#) section on page 17-4.)

Authentication settings represent a different logon and lockout policy from the one that applies when subscribers access Cisco Unity by phone. For information on setting up the account policy that applies when subscribers access to Cisco Unity by phone, see the [“Account Policy Settings”](#) chapter.

Use the following table to learn more about authentication settings.

**Table 28-8 System > Configuration > Authentication Provider Page**

Field	Considerations
Remember Logons for __ Days	<p>If desired, check this check box and enter the number of days that Cisco Unity will store logon information. When you check this check box, logons are stored as encrypted as cookies on the subscriber computer.</p> <p>When Cisco Unity remembers logon information, subscribers do not have to enter it to log on to the Cisco Personal Communications Assistant (PCA). Instead, the logon credentials for a subscriber are automatically populated in the Log On page.</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>Default: Blank.</p>
Remember Passwords for __ Days	<p>If desired, check this check box and enter the number of days that Cisco Unity will store password information. When you check this check box, passwords are stored as encrypted as cookies on the subscriber computer.</p> <p>When Cisco Unity remembers subscriber passwords, subscribers do not have to enter it to log on to the Cisco Personal Communications Assistant (PCA). Instead, a subscriber password is automatically populated in the Log On page.</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>Default: Blank.</p>

Table 28-8 System &gt; Configuration &gt; Authentication Provider Page (continued)

Field	Considerations
Session Key Duration	<p>This field indicates the length of time that the browser can be left unattended before Cisco Unity automatically logs the subscriber off.</p> <p>The value in IIS dictates the browser session duration, but you can use this field to change the value for the Session Timeout field in IIS. When you change the value for the Session Timeout field directly in IIS, however, the changes you make are not reflected here.</p> <p>Regardless of whether you update the session duration here or directly in IIS, the new timeout value applies the next new browser session.</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>Default: 20 minutes.</p>
Disallow Blank Passwords	<p>Check this check box so that subscribers are prohibited from logging on to the Cisco Personal Communications Assistant (PCA) without entering a password in the Log On page, even if the Domino account policy allows blank passwords.</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p>
Lock Out Accounts	<p>Check this check box if you want to specify an account lockout policy for the subscribers using the Cisco Personal Communications Assistant (PCA).</p> <p>When this check box is checked, enter the applicable values in the following fields:</p> <ul style="list-style-type: none"> <li>• Accounts Are Locked Out For __ Minutes</li> <li>• Accounts Will Lock Out After __ Logon Attempts</li> <li>• Reset Account Lockout Counters After __ Minutes</li> </ul> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>Default: Check box checked.</p>
Accounts Are Locked Out For __ Minutes	<p>Enter the number of minutes that Cisco Unity will prevent subscribers from accessing Cisco Unity by using the Cisco Personal Communications Assistant (PCA).</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: 30 minutes.</p>

Table 28-8 System &gt; Configuration &gt; Authentication Provider Page (continued)

Field	Considerations
Accounts Will Lock Out After ___ Logon Attempts	<p>Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by using the Cisco Personal Communications Assistant (PCA).</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: Five attempts.</p>
Reset Account Lockout Counters After ___ Minutes	<p>Enter the number of minutes after which Cisco Unity will clear the count of failed logon attempts to the Cisco Personal Communications Assistant (PCA), unless the failed logon limit is already reached and the account is locked.</p> <p>If IIS is configured so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, this setting also applies to subscribers logging on to the Cisco Unity Administrator and the Status Monitor.</p> <p>This option is unavailable when the Lock Out Accounts check box is unchecked.</p> <p>Default: 30 minutes.</p>

## Voice Messaging Port Settings

Each voice messaging port on the Cisco Unity server can be set to perform one or more of these functions:

- Answer incoming calls from unidentified callers and from subscribers dialing in to Cisco Unity.
- Dial out to notify subscribers of voice, fax, and e-mail messages.
- Dial out to allow system administrators and subscribers to use the phone as a recording and playback device in Cisco Unity applications. (The phone is offered as a recording and playback device in the Media Master, which appears on pages of the Cisco Unity Administrator and Cisco Unity Assistant. The phone is also offered as a playback device in the VCR-style player/recorder available in Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.)

(Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)

- Dial out to turn message waiting indicators (MWIs) on and off.
- Dial out to deliver outbound AMIS messages (some systems may not have this feature).

The number of voice messaging ports set for each of these functions depends on many factors, such as:

- The total number of voice messaging ports available.
- The number of subscribers who will use message notification and how often they will receive notifications.
- For circuit-switched phone systems, whether your integration is serial or analog (analog integrations use a voice messaging port to turn MWIs on and off, while serial integrations do not).
- Whether your organization communicates primarily through e-mail or voice mail.

Each voice messaging port can be set to perform more than one function (for example, to answer calls and to dial out to turn MWIs on). When the voice messaging ports perform more than one function and are very active (for example, answering many calls), the other functions may be delayed until the voice messaging port is free (for example, MWIs cannot be turned on until there are fewer calls to answer). For guidelines on setting up the voice messaging ports, see [Table 28-9](#). For best performance, use the first voice messaging ports for incoming calls and the last ports to dial out. This helps minimize the possibility of a collision, in which an incoming call arrives on a port at the same time that Cisco Unity takes the port off-hook to dial out.

In a typical installation, the installer sets up voice messaging ports for Cisco Unity, but you can modify them on the Ports page. Before changing port settings, however, monitor the voice messaging port activity. Refer to the Port Usage Analyzer, available in Tools Depot.

Use the following table to learn more about port settings.

**Table 28-9 System > Ports Page**

Field	Considerations
Extension	Enter the extension for the port as assigned on the phone system.
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.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from unidentified callers or from subscribers. As a general guideline, set Answer Calls on approximately 75 percent of the ports.
Message Notification	Check this check box to designate the port for notifying subscribers of messages. Assign Message Notification to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.
Dialout MWI <i>(not used by serial or SMDI integrations)</i>	Check this check box to designate the port for turning MWIs on and off. Assign Dialout MWI to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.
TRAP Connection	Check this check box so that subscribers can use the phone as a recording and playback device in Cisco Unity web applications and e-mail clients. Assign TRAP Connection to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.

## Cisco CallManager Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.

Use the following table to learn more about the integration settings.

**Table 28-10 System > Integration > Cisco CallManager Page**

Field	Considerations
Integration Name	<i>Display only.</i> This field displays the name of the Cisco CallManager integration entered in UTIM.
Manufacturer	<i>Display only.</i> This field displays the phone system manufacturer selected in UTIM.
Model	<i>Display only.</i> This field displays the phone system model selected in UTIM.
Software Version	<i>Display only.</i> This field displays the phone system software version selected in UTIM.
Trunk Access Code (for dual phone system integrations only)	<i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM.
Cluster Name	<i>Display only.</i> This field displays the name of the Cisco CallManager cluster entered in UTIM.
IP Address/Name	<i>Display only.</i> This field displays the IP address of the publisher (primary) Cisco CallManager server. This address was entered in UTIM.
IP Port	<i>Display only.</i> This field displays the TCP port used by the Cisco CallManager servers. This port was entered in UTIM.
RTP/IP Port Base	<i>Display only.</i> This field displays the first (or base) port number for RTP used by the Cisco CallManager servers. This first port number was entered in UTIM.
Reconnect	<i>Display only.</i> This field displays whether Cisco Unity will automatically reconnect to the publisher (primary) Cisco CallManager server after failover has been corrected. The setting True indicates that automatic reconnection is enabled. This value was set in UTIM.
IP Addresses	<i>Display only.</i> This field displays the IP addresses of the subscriber (secondary) Cisco CallManager servers. These addresses were entered in UTIM.
MWI On Extension	<i>Display only.</i> This field displays the extension that Cisco CallManager uses to turn MWIs on. This extension was entered in UTIM.
MWI Off Extension	<i>Display only.</i> This field displays the extension that Cisco CallManager uses to turn MWIs off. This extension was entered in UTIM.
Resynchronize At	<i>Display only.</i> This field displays the time each day that Cisco Unity resynchronizes MWIs for every subscriber account. This time was entered in UTIM. Resynchronization occurs only when it is enabled in UTIM.
Number of Ports	<i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the Cisco CallManager server.
CallManager Device Name Prefix	<i>Display only.</i> This field displays the prefix Cisco CallManager adds to the device name for the voice messaging ports. This prefix was entered in UTIM and must match the prefix used by Cisco CallManager.

## SIP Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.

Use the following table to learn more about the integration settings.

**Table 28-11 System > Integration > SIP Page**

Field	Considerations
Integration Name	<i>Display only.</i> This field displays the name of SIP integration entered in UTIM.
Manufacturer	<i>Display only.</i> This field displays the phone system manufacturer selected in UTIM.
Model	<i>Display only.</i> This field displays the phone system model selected in UTIM.
Software Version	<i>Display only.</i> This field displays the phone system software version selected in UTIM.
Trunk Access Code <i>(for dual phone system integrations only)</i>	<i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM.
Cluster Name	<i>Display only.</i> This field displays the name of the SIP cluster entered in UTIM.
IP Address/Name	<i>Display only.</i> This field displays the IP address of the primary SIP proxy server. This address was entered in UTIM.
IP Port	<i>Display only.</i> This field displays the IP port used by the primary SIP proxy server. This port was entered in UTIM.
IP Addresses	<i>Display only.</i> This field displays the IP addresses of the secondary SIP proxy servers. These addresses were entered in UTIM.
Authentication <i>(only when authentication is enabled)</i>	<i>Display only.</i> This field displays whether Cisco Unity authenticates with the SIP proxy server. The setting True indicates that authentication is enabled. This value was set in UTIM.
Name <i>(only when authentication is enabled)</i>	<i>Display only.</i> This field displays the name the SIP proxy server uses for authentication. This name was entered in UTIM.
Contact Line Name	<i>Display only.</i> This field displays the voice messaging line name that subscribers use to contact Cisco Unity. This line name was entered in UTIM.
Starting RTP Audio Port	<i>Display only.</i> This field displays the first RTP audio port that subscribers use to contact Cisco Unity. This first RTP audio port was entered in UTIM.
Preferred Codec	<i>Display only.</i> This field displays the preferred codec that subscribers use when contacting Cisco Unity. This codec was selected in UTIM.
Number of Ports	<i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the SIP proxy server.

## Circuit-Switched Integration

The integration settings are specified during installation in the Cisco Unity Telephony Integration Manager (UTIM), which configures Cisco Unity to work with the specified phone system. Once the integration is set up, you should not need to change the integration settings, but you can review them on the Integration page or revise them in UTIM.

Use the following table to learn more about the integration settings.

**Table 28-12 System > Integration > Circuit-Switched Page**

Field	Considerations
Integration Name	<i>Display only.</i> This field displays the name of integration entered in UTIM.
Manufacturer	<i>Display only.</i> This field displays the phone system manufacturer selected in UTIM.
Model	<i>Display only.</i> This field displays the phone system model selected in UTIM.
Software Version	<i>Display only.</i> This field displays the phone system software version selected in UTIM.
Trunk Access Code <i>(for dual phone system integrations only)</i>	<i>Display only.</i> This field displays the number that Cisco Unity dials to transfer a call from one phone system to the other. This code was entered in UTIM.
MWI On Code <i>(for analog or DTMF integrations only)</i>	<i>Display only.</i> This field displays the code that the phone system uses to turn MWIs on. This code was entered in UTIM.
MWI Off Code <i>(for analog or DTMF integrations only)</i>	<i>Display only.</i> This field displays the code that the phone system uses to turn MWIs off. This code was entered in UTIM.
SMDI Field Length <i>(for serial or SMDI integrations only)</i>	<i>Display only.</i> This field displays the SMDI or station field length for the phone system. The SMDI field length is the length of the SMDI or station prefix plus the default extension length. The length is either 10 or 7. This value was entered in UTIM and must match the settings used by the phone system.  SMDI serial integrations use SMDI packets to send information about the call. The information in an SMDI packet varies according to the phone system, but the packet may include ANI, DNIS, call type (forward or direct), and forwarding station.
Default Extension Length <i>(for serial or SMDI integrations only)</i>	<i>Display only.</i> This field displays the default length of extensions on the phone system. This length was selected in UTIM.
Resynchronize At	<i>Display only.</i> This field displays the time each day that Cisco Unity resynchronizes MWIs for every subscriber account. This time was entered in UTIM. Resynchronization occurs only when it is enabled in UTIM.
Serial Communication Settings: <ul style="list-style-type: none"> <li>• COM Port</li> <li>• Baud Rate</li> <li>• Data Bits</li> <li>• Stop Bits</li> <li>• Parity</li> </ul> <i>(for serial or SMDI integrations only)</i>	<i>Display only.</i> The fields in this section show the serial communication settings used in SMDI serial integrations. These settings are disabled for other types of integrations.  The COM Port field setting specifies the communications port on the Cisco Unity server. The Baud, Data Bits, Stop Bits, and Parity field settings must match the serial communication settings used by the phone system.
Number of Ports	<i>Display only.</i> This field displays the number of voice messaging ports set up in UTIM to connect Cisco Unity to the phone system.

# Setting a Warning Tone for End of Recording

This feature applies only to integrations with Cisco CallManager and SIP phone systems.

Cisco Unity can be set to sound a warning tone before reaching the maximum allowable message length while callers record their messages. You can also customize the warning tone by recording a WAV file with another tone or a brief message.

## Enabling the Warning Tone

By default, the warning tone is disabled. There are two settings that can be customized:

- The number of milliseconds before reaching the maximum message length when the warning tone will sound. Any setting greater than 0 enables the warning tone.
- The maximum recording length in milliseconds for which no warning tone will sound. This setting prevents the warning tone from sounding for shorter recordings such as voice names.

For example, if the maximum message length is set for 300 seconds and the first setting is set for 10 seconds, the warning tone will sound after 290 seconds of recording—10 seconds before the recording limit is reached and the recording session is terminated.

To enable the warning tone, do the following procedure.

### To Enable the Warning Tone for the End of Recording

- 
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
  - Step 2** In the left pane, expand **Administrative Tools**, and double-click **Advanced Settings Tool**.
  - Step 3** In the Unity Settings pane, click **Conversation – Record Termination Warning: Record Termination Warning Time**. Information about this setting appears in the Description box.
  - Step 4** In the New Value field, enter a number of milliseconds to indicate when the warning tone will sound. The tone sounds this number of milliseconds prior to the end of the allowed recording time. We recommend entering **10000**.
  - Step 5** Click **Set**.
  - Step 6** In the Unity Settings pane, click **Conversation – Record Termination Warning: Minimum Recording Length for Termination Warning**.
  - Step 7** In the New Value field, enter the maximum recording length in milliseconds for which no warning tone will sound. We recommend entering **30000**.
  - Step 8** Click **Set**.
  - Step 9** Click **Exit** to close the Unity Registry Settings window.
  - Step 10** For the settings to take effect, exit and restart the Cisco Unity software.
- 

## Customizing the Warning Tone

By default, the recording beep sounds as the warning tone. You can customize the warning tone by recording another tone or a brief message as a WAV file and specifying the location of the WAV file.

To specify a customized warning tone, do the following procedure.

#### To Specify the Location of a Customized Warning Tone

- 
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, expand **Administrative Tools**, and double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Conversation – Record Termination Warning: Warning WAV File Location**.
- Step 4** In the New Value field, enter the full path of the WAV file that you want to use as the warning tone.
- Step 5** Click **Set**.
- Step 6** Click **Exit** to close the Unity Registry Settings window.
- Step 7** For the settings to take effect, exit and restart the Cisco Unity software.
- 

## Remapping Extension Numbers

This section provides the following information on remapping extension numbers:

- [About the Remapping Feature, page 28-20](#)
- [Setting Up Cisco Unity to Remap Extension Numbers, page 28-20](#)
- [Syntax and Examples, page 28-22](#)

## About the Remapping Feature

The extension remapping feature lets you convert to the extensions of your choice the calling numbers and forwarding numbers of calls handled by Cisco Unity. This feature is useful, for example, when the phone system cannot map multiple extension numbers on a subscriber phone to a single Inbox.

Remapping can change one or both of the following extension numbers in a call:

- Calling number (the number from which a call originates). For example, Cisco Unity changes the calling number of calls so that the caller ID appears to be a different extension than the one that actually placed the call.
- Forwarding number (the number that a call is going to). For example, unanswered calls to all line extensions on a single phone can be forwarded to the Inbox of a single subscriber; or unanswered calls to phones not assigned to subscribers can be forwarded to the Inbox of a supervisor.

## Setting Up Cisco Unity to Remap Extension Numbers

This section includes a procedure for enabling the remapping feature. You can create multiple files in either or both of two directories:

- In the Calling directory, one or more .exm files remap caller ID numbers.
- In the Forwarding directory, one or more .exm files remap numbers that Cisco Unity provides with calls it forwards.

When you create remapping instructions in a .exm file in a directory, Cisco Unity remaps only the type of extension number that the directory is named for. For example, if you want to remap only the extensions that Cisco Unity provides with calls it forwards, you enter the instructions in a .exm file in the Forwarding directory; in this circumstance, the Calling directory needs no .exm file.

In each directory, you can have several .exm files with different file names but with the same .exm extension. This helps you to organize the remapping information. For example, you could create two files in a directory: Ports\_1-12.exm and Ports\_13-24.exm. Cisco Unity reads all files that have the .exm extension in these directories.

### To Remap Extension Numbers

---

- Step 1** On the Cisco Unity server, browse to the CommServer\IntLib\ExtensionMapping directory. In this directory is the file Sample.txt and two more directories: Calling and Forwarding.
- Step 2** To remap calling numbers, go to the Calling directory.
- Step 3** In a text editor application, create a new .exm file, or open a currently existing .exm file.  
For an example, open the file **Sample.txt** in the CommServer\IntLib\ExtensionMapping directory.
- Step 4** Enter **[Range]** and press **Return** to create a section for indicating which voice messaging ports will be monitored for remapping calls.  
A .exm file can have only one [Range] section.
- Step 5** Enter **ports=** followed by the numbers of the voice messaging ports, separated by commas. Ranges are designated by a hyphen (-) without spaces. To monitor all voice messaging ports, enter **ports=\*** on this line. Then press **Return**.  
For example, you might enter:  
ports=1,2,5-34
- Step 6** To create a section for the remapping rules, press **Return**, enter **[Number Mappings]**, and then press **Return**.  
A .exm file can have only one [Number Mappings] section.
- Step 7** Enter one remapping rule on the line, and then press **Return**.  
See the remapping rule examples in the following “[Syntax and Examples](#)” section. The rule format is:  
<original number>, <new number>  
The rules cannot include spaces between digits. However, the numbers must be separated by a comma and a single space. Wildcard characters cannot appear at the beginning of a number.
- Step 8** For all remaining rules, repeat [Step 7](#).
- Step 9** Save and close the .exm file.
- Step 10** To remap forwarding numbers, browse to the directory CommServer\IntLib\ExtensionMapping\Forwarding.
- Step 11** Repeat [Step 3](#) through [Step 9](#) to remap forwarding numbers.
- Step 12** For extension remapping to take effect, restart the Cisco Unity software.
-

## Syntax and Examples

Table 28-13 shows the wildcard characters you can use in the .exm files.

**Table 28-13 Wildcard Characters**

Wildcard	Result
*	Matches zero or more digits.
?	Matches exactly one digit. Use ? as a placeholder for a single digit.

Table 28-14 gives examples for the syntax and results of rules in the .exm files.

**Table 28-14 Syntax Examples**

Rule	Original Number	New Number
2189, 1189	2189	1189
3189, 1189	3189	1189
4189, 1189	4189	1189
2???, 1???	2189	1189
	2291	1291
3???, 1???	3189	1189
	3291	1291
8???, 61???	8000	61000
	8765	61765
123*, 44*	12300	4400
	12385	4485

Cisco Unity executes rules in the order they appear in the .exm file. For example, the .exm file might contain the following rules:

```
1234, 1189
3189, 1189
4189, 1189
123?, 8891
```

The extension 1234 would be remapped to 1189 while extensions 1233 and 1235 would be remapped to 8891, because the rule mapping 1234 appears earlier.

An .exm file might contain the following:

```
[Range]
ports=1,2,5-34
```

```
[Number Mappings]
2189, 1189
3189, 1189
4189, 1189
8???, 9???
```







## GLOSSARY

---

### A

- account policy** The collection of settings that govern passwords and lockouts for all Cisco Unity accounts.
- Cisco Unity Assistant** The Web interface that gives subscribers the ability to customize personal settings—including recorded greetings and message delivery options—on their computers. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.)
- alternate extension** The addition number(s) assigned to a subscriber. Used when setting up Digital Networking, when handling multiple line appearances on subscriber phones, or as a convenience for subscribers and callers who want to communicate by using a cell phone, home phone, or phone at an alternate work site in addition to a subscriber phone. *See also* [extension](#) and [primary extension](#).
- alternate greeting** A substitute recording that can be turned on and off; it is used for a variety of special situations, such as vacations or a holiday. When active, the alternate greeting overrides all other greetings.
- ANI** Automatic number identification. The detection of the digits in a calling phone number.
- audiotext** Prerecorded information that an organization makes available to callers.
- automated attendant** A call handler that is used in place of a human operator to answer and direct calls by playing greetings and responding to touchtones.
- automatic number identification** *See* [ANI](#).

---

### B

- busy greeting** The recording that plays when a subscriber extension is busy.

---

### C

- call handler** A tool for managing calls in Cisco Unity; it answers calls and handles them according to the call handler settings. *See also* [Goodbye call handler](#), [Opening Greeting call handler](#), and [Operator call handler](#).
- call routing table** A tool for managing calls in Cisco Unity. A call routing table consists of a collection of rules that define how calls are routed; Cisco Unity compares call information with the rules in a table, then routes the call according to the first matching rule. Rules can be based on the call type (internal, external), forwarding station, phone numbers of callers, trunks or ports on which calls come in, dialed phone numbers, and schedules.

<b>call screening</b>	The Cisco Unity function of recording the name of a caller and playing it for the subscriber, who can choose whether to take the call.
<b>call transfer</b>	The Cisco Unity function of routing unidentified callers to a phone or to the greetings of a subscriber or handler. Call transfer settings also specify how Cisco Unity handles a transfer: Cisco Unity can either release the call to the phone system, or it can supervise the transfer. <i>See also</i> <a href="#">release to switch</a> , <a href="#">supervised transfer</a> , and <a href="#">unidentified caller</a> .
<b>caller input</b>	Information a caller enters by pressing phone keys to dial an extension, spell a name, or select an option during the Cisco Unity conversation.
<b>calling extension</b>	The extension from which a call originates.
<b>calling number</b>	The phone number from which a call originates.
<b>Cisco Unity Administrator</b>	A Web administrator that allows you to access Cisco Unity via an intranet and remotely. Use the Cisco Unity Administrator to create or modify subscriber accounts, configure messaging options, assign classes of service, record greetings, and run reports.
<b>Cisco Unity conversation</b>	The set of prerecorded instructions and options that Cisco Unity plays over the phone to subscribers and other callers; it consists of the subscriber conversation and the unidentified caller conversation. <i>See</i> <a href="#">unidentified caller</a> and <a href="#">unidentified caller conversation</a> .
<b>Cisco Unity server</b>	The computer that runs the Cisco Unity software.
<b>class of service</b>	<i>See</i> <a href="#">COS</a> .
<b>closed greeting</b>	The recording that plays during the closed hours for the active schedule.
<b>closed hours</b>	The hours and days in a schedule that have not been identified as standard hours; these are typically nonbusiness hours.
<b>codec</b>	An analog-to-digital coder/decoder; also referred to as a converter.
<b>conversation</b>	<i>See</i> <a href="#">Cisco Unity conversation</a> .
<b>COS</b>	Class of service. A collection of permissions and restrictions assigned to each subscriber that control access to and use of the system.

---

## D

<b>dialed extension</b>	The extension that a caller dials.
<b>dialed number</b>	The phone number that a caller dials.
<b>dialed number identification service</b>	<i>See</i> <a href="#">DNIS</a> .
<b>DID</b>	Direct inward dialing. A phone system function in which calls are routed directly to specific extensions without first being routed by an attendant.
<b>Digital Networking</b>	The Cisco Unity feature that enables subscribers to send and receive voice messages between Cisco Unity servers.

<b>direct call</b>	Internal calls from subscribers and external calls from unidentified callers that are routed to Cisco Unity by the phone system.
<b>directory assistance</b>	The audio listing provided by a directory handler that callers can use to reach subscribers and to leave messages.
<b>directory handler</b>	A tool for managing calls in Cisco Unity; it provides directory assistance and contains settings that define how callers can search for subscriber names and/or extensions and what Cisco Unity does when a match is made.
<b>distribution list</b>	See <a href="#">public distribution list</a> .
<b>DNIS</b>	Dialed number identification service. In North America, the detection of the dialed number on an 800 or 900 line.
<b>DTMF</b>	Dual-tone multifrequency. Phone system signaling in which standard pairs of specific voice band frequencies are used; it is also referred to as touchtone dialing.
<b>DTMF extension</b>	The touchtones that correspond to an extension.
<b>dual-tone multifrequency</b>	See <a href="#">DTMF</a> .

---

## E

<b>easy message access</b>	A feature that allows a subscriber to retrieve messages from the Cisco Unity conversation without entering an ID. Depending on the phone system integration, Cisco Unity can identify a subscriber based on the extension from which the call originated. A password may be required.
<b>enrollment</b>	See <a href="#">subscriber enrollment</a> .
<b>extension</b>	The DTMF ID that is assigned to each subscriber when their Cisco Unity accounts are created; typically, this ID is the internal phone number that rings a subscriber phone. Also called the primary extension. See also <a href="#">alternate extension</a> and <a href="#">primary extension</a> .

---

## F

<b>forwarded call</b>	Internal calls from subscribers and external calls from unidentified callers that are forwarded to Cisco Unity from an extension.
-----------------------	---

---

## G

<b>Goodbye call handler</b>	A predefined call handler that plays a brief goodbye message and then hangs up.
<b>greeting</b>	A recording that welcomes callers and offers menu options or the opportunity to leave a message. Greetings can be recorded by subscribers, system administrators, or voice talent.

---

**H**

**handlers** The group of tools that Cisco Unity uses to manage calls. *See also* [call handler](#), [call routing table](#), [directory handler](#), [interview handler](#), and [restriction table](#).

---

**I–J**

**ID** A numeric identifier that Cisco Unity uses to recognize a subscriber. A subscriber ID usually is the extension assigned to a subscriber.

**Inbox** The receptacle in which an e-mail application stores incoming messages.

**internal greeting** The recording that a subscriber can set up to play only to other subscribers in place of the standard or alternate greeting.

**Internet subscriber** A type of Cisco Unity subscriber who does not have a local message store but instead sends and receives messages by using an Internet Mail Service (SMTP gateway).

**interview handler** A tool for managing calls in Cisco Unity; it is used to collect information from callers by playing a series of recorded questions, and then recording their answers.

---

**K**

**keypad** The portion of a phone that contains touchtone keys.

**keypad map** The numeric keys to which Q and Z are assigned on a phone keypad.

---

**L**

**LDAP** Lightweight Directory Access Protocol. A format used to provide access to information directories; supports TCP/IP.

**license files** For Cisco Unity 4.0 and later, files that contain information on the number of ports and optional packages purchased for the system; Cisco Unity checks the license files to activate the correct options. Beginning with Cisco Unity 4.0, license files replace the system key.

**Lightweight Directory Access Protocol** *See* [LDAP](#).

**listing status** The status of a subscriber in directory assistance; a subscriber can be Listed or Not Listed.

**location** A Cisco Unity object that contains the addressing information that Cisco Unity needs to exchange messages with other voice messaging systems (which may or may not be Cisco Unity systems). Each Cisco Unity server is associated with one location, called the primary location, which is created during installation and which cannot be deleted.

---

**M**

<b>Media Master control bar</b>	The VCR-style recording and playback device that appears on several pages of the Cisco Unity Administrator and the Cisco Unity Assistant. It can be used to record and play names, messages, and greetings, either with a phone or with a computer microphone and speakers. (Subscribers use a similar, VCR-style recording and playback controls in Lotus Notes with IBM Lotus Domino Unified Communications Services (DUCS) for Cisco Unity.)
<b>member</b>	A subscriber assigned to a class of service, or a subscriber or public distribution list that is included in another public distribution list or in a private list.
<b>message notification</b>	The Cisco Unity function of notifying a subscriber when new messages arrive.
<b>message summary</b>	Information about a message, including sender, special delivery status, time and date sent, and copy recipients. Subscribers can choose to hear a message summary before or after the message plays, or not at all.
<b>MWI</b>	Message waiting indicator. A phone system device (lamp, distinctive dial tone, or LCD display) that alerts a subscriber to the arrival of new messages.

---

**N**

<b>navigation bar</b>	The area of the Cisco Unity Administrator and of the Cisco Unity Assistant that contains links to categories of data pages.
<b>NDR</b>	Nondelivery receipts. An NDR message informs the sender when a voice message cannot be delivered to its intended recipient.
<b>new message</b>	A message that has not been heard by a subscriber.

---

**O**

<b>old message</b>	A message that has been heard by a subscriber. Old messages include saved messages and deleted messages.
<b>Opening Greeting call handler</b>	A predefined call handler that acts as an automated attendant, playing the greeting that callers first hear when they call the organization, and performing specified actions.
<b>Operator call handler</b>	A predefined call handler that calls are routed to when callers press “0” or do not press any key as requested in the Cisco Unity conversation.

---

**P–Q**

<b>primary extension</b>	The DTMF ID that is assigned to each subscriber when their Cisco Unity accounts are created; typically, this ID is the internal phone number that rings a subscriber phone. <i>See also</i> <a href="#">alternate extension</a> and <a href="#">extension</a> .
--------------------------	---

<b>private distribution list</b>	A list of message recipients (subscribers and/or public distribution lists) used to send voice messages to more than one subscriber at a time. The individual subscriber who owns the list is the only person who can add and remove members from the list, and the only one who can use the list.
<b>prompt</b>	A recorded instruction, statement, or question in the Cisco Unity conversation.
<b>public distribution list</b>	A list of message recipients (subscribers and/or public distribution lists) used to send voice messages to more than one subscriber at a time. Anyone can send messages to public distribution lists, which are created and maintained by an administrator.

---

## R

<b>record</b>	The group of settings or collection of data for an individual subscriber, class of service, or other Cisco Unity entity.
<b>recorded name</b>	A recording of the name of a subscriber; also called voice name.
<b>release to switch</b>	A call transfer type in which Cisco Unity puts the caller on hold, dials the extension, and releases the call to the phone system. When the line is busy or is not answered, the phone system—not Cisco Unity—forwards the call as specified.
<b>restriction table</b>	A tool for managing calls in Cisco Unity. A restriction table consists of a collection of dial strings that permit or restrict the phone numbers that subscribers and administrators can use for transferring calls, for sending message notification, and for delivering faxes.
<b>routing table</b>	<i>See</i> <a href="#">call routing table</a> .
<b>RTP</b>	The Real-Time Transport Protocol (RTP) is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data (audio and video) over packet switched networks. It is used by both SIP and H.323.

---

## S

<b>saved message</b>	A message that has been heard and stored by a subscriber.
<b>SMTP</b>	Simple Mail Transfer Protocol. A format used to send e-mail messages between servers.
<b>standard greeting</b>	A recording that plays during the standard hours specified for the active schedule.
<b>standard hours</b>	The hours and days in a schedule that are designated as business hours.
<b>Status Monitor</b>	A Web-based application on the Cisco Unity server that contains pages providing information about system status, ports, reports, and disk drives; also used to start and to shut down Cisco Unity.
<b>subscriber</b>	Anyone enrolled on Cisco Unity.
<b>subscriber conversation</b>	The set of prerecorded instructions and options that Cisco Unity plays over the phone to subscribers, enabling them to send messages, hear messages, and change settings.
<b>subscriber enrollment</b>	The process of preparing a subscriber account for use: recording a name and greeting, setting a password, and choosing whether the subscriber is listed in the directory.

<b>subscriber template</b>	A collection of settings that are common to a group of subscribers and that are applied when a subscriber account based on the template is created. Settings include schedules, passwords, account permissions, call processing and transfer options, and distribution lists.
<b>summary</b>	See <a href="#">message summary</a> .
<b>supervised transfer</b>	A call transfer type in which Cisco Unity acts as a receptionist, handling the transfer. If the line is busy or the call is not answered, Cisco Unity—not the phone system—forwards the call as specified.
<b>system key</b>	Prior to Cisco Unity 4.0, the device programmed with the number of ports and optional packages purchased for the system; Cisco Unity checked the system key to activate the correct options. Beginning with Cisco Unity 4.0, license files replace the system key.

---

## T

<b>TRAP</b>	Telephone Recording and Playback. The feature that allows subscribers to use the phone as the recording and playback device for the Media Master control bar as an alternative to using a computer microphone and speakers. See also <a href="#">Media Master control bar</a> .
<b>touchtone keys</b>	The 12 buttons with letters, numbers, and/or characters on a phone keypad; callers press keys to dial extensions, spell names, and select options in the Cisco Unity conversation.

---

## U

<b>UDP</b>	User Datagram Protocol is a lightweight transport built on top of IP. UDP obtains extra performance from IP by not implementing some of the features of TCP. Specifically, UDP allows individual packets to be dropped without retries, and UDP packets can be received in a different order than they were sent.
<b>UMR</b>	<p>All messages from outside callers are temporarily stored on the Cisco Unity server—in the Unity Message Repository (UMR)—before they are forwarded for storage in the subscriber mailbox. This allows Cisco Unity to continue functioning when the network connection is down between the Cisco Unity server and the Domino servers, or when one or more Domino servers are down.</p> <p>While Domino or the network is off line, Cisco Unity can still answer calls, allow outside callers to look up subscriber extensions, and record voice messages. During this time, subscribers who check their voice messages hear the UMR conversation, which explains that their Domino server is not available, but lets them access voice messages left from the time that it went down. When the Domino server or network is back on line, the voice messages stored in the messaging repository are routed to the subscriber mailboxes. (In some cases when a network connection or mail server is down, subscriber-to-subscriber messages are also treated as outside caller messages and stored on the Cisco Unity server until they can be delivered to the applicable mailbox.)</p>
<b>unidentified caller</b>	An external caller or a subscriber who has not entered a Cisco Unity ID when calling from outside an organization, or a subscriber who has not entered an ID when calling from inside the organization on a phone system that does not support identified subscriber messaging. See <a href="#">unidentified caller conversation</a>
<b>unidentified caller conversation</b>	The set of prerecorded instructions and options that Cisco Unity plays over the phone to unidentified callers, enabling them to reach subscribers, select options, get information about an organization, and leave messages. See <a href="#">conversation</a> .

**unified messaging** A messaging system in which all types of messages can be managed from the same Inbox.

---

## **V-Z**

**virtual private network** A private network that uses public phone lines (or in some cases a cable modem). Privacy is maintained through encryption and the use of secure protocols. Also referred to as a VPN.



# Exiting and Starting the Cisco Unity Software and Server

The following sections provide instructions on exiting the Cisco Unity software, shutting down and restarting the Cisco Unity server, and starting the Cisco Unity software.

## Exiting the Cisco Unity Software

This section provides two procedures for exiting the software: from the Cisco Unity server and from another computer. (For details on the accounts that you use to log on to the Cisco Unity server and the Cisco Unity Status Monitor, see the [“About the Accounts That Can Be Used to Administer Cisco Unity” section on page 2-11.](#))



### Caution

Do not use `Kill av*.*` to exit the Cisco Unity software. `Kill av*.*` does not stop all Cisco Unity services, and may cause problems with upgrades from Cisco Unity version 2.x.

### To Exit the Cisco Unity Software from the Cisco Unity Server

- Step 1** If the system uses the automated attendant, route all calls to the operator.
- Step 2** Log on to Windows on the Cisco Unity server by using either the administration account or an applicable Windows domain account.
- Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar.  
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)
- Step 4** Click **Stop Cisco Unity**. Cisco Unity stops running when all calls are finished, and an “X” appears in the Cisco Unity icon.
- Step 5** Press **Ctrl-Alt-Delete**, then lock or log off Windows to prevent access by unauthorized users.

### To Exit the Cisco Unity Software from Another Computer

- Step 1** If the system uses the automated attendant, route all calls to the operator.

- Step 2** When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following sub-steps. Otherwise, proceed to [Step 3](#).
- Log on to Windows by using either the administration account or an applicable Windows domain account.
  - Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
  - If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or an applicable Windows domain account.
  - Proceed to [Step 6](#).
- Step 3** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following:
- Log on to Windows by using any domain account that has the right to log on locally.
  - Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 4** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an applicable Cisco Unity subscriber account, and proceed to [Step 6](#).
  - Click **Log On Using Windows Authentication**.
- Step 5** On the Cisco Unity Log On page, enter the user name, password, and domain for the administration account or an applicable Windows domain account.
- Step 6** In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:
- Cisco Unity stops running after all calls are finished.
  - Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.
- Step 7** Click **Shut Down**.
- 

## Shutting Down or Restarting the Cisco Unity Server



### Note

If an expansion chassis is connected to the Cisco Unity server and both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.

---

### To Shut Down or Restart the Cisco Unity Server

---

- Step 1** Exit the Cisco Unity software, if it is running, by using a procedure in the “[Exiting the Cisco Unity Software](#)” section on page A-1.
- Step 2** On the Windows Start menu, click **Shut Down**.

**Step 3** Click **Shut Down** or **Restart**.

During a restart, the Cisco Unity software starts automatically.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.

When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon in the status area of the taskbar.

## Starting the Cisco Unity Software

This section provides two procedures for starting the software: from the Cisco Unity server and from another computer. (For details on the accounts that you use to log on to the Cisco Unity server and the Cisco Unity Status Monitor, see the [“About the Accounts That Can Be Used to Administer Cisco Unity” section on page 2-11.](#))

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the following procedures only if you exited the Cisco Unity software but did not restart the server.

Domino must be running on the server that Cisco Unity connects with before you start the Cisco Unity software.

If Domino stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

### To Start the Cisco Unity Software from the Cisco Unity Server

**Step 1** Log on to Windows on the Cisco Unity server by using either the administration account or an applicable Windows domain account.

**Step 2** Right-click the **Cisco Unity** icon in the status area of the taskbar.

(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)

**Step 3** Click **Start Cisco Unity**.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.

When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon.

**Step 4** Press **Ctrl-Alt-Delete**, then lock or log off Windows to prevent access by unauthorized users.

**Step 5** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.

---

**To start the Cisco Unity software from another computer**

- 
- Step 1** When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following sub-steps. Otherwise, proceed to [Step 2](#).
- a. Log on to Windows by using either the administration account or an applicable Windows domain account.
  - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
  - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or an applicable Windows domain account.
  - d. Proceed to [Step 5](#).
- Step 2** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following:
- a. Log on to Windows by using any domain account that has the right to log on locally.
  - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an applicable Cisco Unity subscriber account (if there is one), and proceed to [Step 5](#).
  - Click **Log On Using Windows Authentication**.
- Step 4** On the Cisco Unity Log On page, enter the user name, password, and domain for the administration account or an applicable Windows domain account.
- Step 5** In the Cisco Unity Status Monitor, click the **System Status** icon (the first icon), at the top of the page.
- Step 6** Click **Start**.
- Step 7** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-



## A

- account lockouts
  - security policy for accessing Cisco Unity by phone [19-3](#)
  - security policy for GUI access [28-11](#)
- account policy
  - account lockout settings for GUI access [28-11](#)
  - account lockout settings for phone access [19-3](#)
  - overview for phone access [19-1](#)
  - password settings for GUI access [28-11](#)
  - phone password settings [19-1](#)
- accounts
  - Cisco Unity Admin, installing [6-1](#)
  - Cisco Unity Messaging System [6-2](#)
  - deleting [16-1](#)
  - Example Administrator [6-1](#)
  - Example Subscriber [6-2](#)
  - subscriber, creating [15-1](#)
- account settings
  - subscriber [17-4](#)
  - subscriber template [13-4](#)
- ActiveAssistant (AA). See Cisco Unity Assistant
- Add icon [3-3](#)
- adding
  - alternate extensions [17-26](#)
  - call handlers [21-3](#)
  - call routing rules [22-2, 24-3](#)
  - classes of service [14-2](#)
  - distribution lists [18-2](#)
  - holidays [28-10](#)
  - interview handlers [23-2](#)
  - languages [11-1](#)
  - public distribution lists [18-2](#)
  - records [3-4](#)
  - restriction tables [25-3](#)
  - schedules [28-9](#)
  - subscribers, with Bulk Import wizard [15-15](#)
  - subscribers, with Cisco Unity Administrator [15-16](#)
  - subscribers to a class of service [14-3](#)
  - subscribers to a public distribution list [18-4](#)
  - subscriber templates [13-2](#)
- Address Books
  - adding [28-7](#)
  - importing from to create subscribers [28-7](#)
- addressing
  - messages, spelling vs. number modes [7-9, 9-3](#)
  - setting options for primary location [27-3](#)
- administration account
  - limiting use of [2-11](#)
  - using to log on to the Cisco Unity Administrator [2-11](#)
- Administrative Access Activity report [26-8](#)
- administrative rights, granting [2-15](#)
- administrator accounts [6-1](#)
- Advanced Settings tool
  - activating Optional Conversation 1 [7-4](#)
  - enabling warning tone for end of recording [28-19](#)
- All Subscribers public distribution list [18-1](#)
- alternate extensions [17-25](#)
- ANI playback [7-6](#)
- Anonymous authentication
  - advantages and disadvantages of [2-5](#)
  - how it works with the Cisco Unity Administrator [2-8](#)
- authentication
  - how it works with Cisco Personal Communications Assistant [8-4](#)
  - Integrated Windows authentication [2-5](#)

method for Cisco Unity Administrator [2-5](#)  
 overview for Cisco Personal Communications Assistant [8-4](#)  
 overview for Cisco Unity administrator [2-5](#)  
 automated attendant [9-4](#)

---

## B

billing ID [13-4](#)  
 browser language [11-5](#)  
 Bulk Edit utility  
   modifying multiple call handlers [21-2](#)  
   modifying multiple subscribers [15-18, 17-1](#)  
 Bulk Import wizard  
   creating subscribers [15-5](#)  
   errors, correcting [15-15](#)  
   overview [15-5](#)

---

## C

caller input settings  
   call handler [21-12](#)  
   directory handler [22-8](#)  
   subscriber [17-16](#)  
   subscriber template [13-13](#)  
 call handler greetings, changing by phone [21-2](#)  
 call handlers  
   automated attendant [21-1](#)  
   caller input settings [21-12](#)  
   class of service access settings [14-5](#)  
   deleting owner [16-1](#)  
   Goodbye [21-2](#)  
   greetings settings [21-10](#)  
   messages settings [21-13](#)  
   names, recording [3-5, 7-10](#)  
   Opening Greeting [21-2](#)  
   Operator [21-2](#)  
   orphans, avoiding [16-1](#)  
   predefined [21-2](#)

  profile settings [21-5](#)  
   settings overview [21-1](#)  
   traffic report [26-11](#)  
   transfer settings [21-7](#)  
 Call Handler Traffic report [26-11](#)  
 call management  
   creating a map [20-2](#)  
   planning [20-2](#)  
   tools overview [20-1](#)  
 CallManager integration settings [28-15](#)  
 call routing  
   call management map [20-2](#)  
   one key dialing [20-2](#)  
 call routing rules  
   adding [22-2, 24-3](#)  
   settings [24-4](#)  
 call routing tables  
   class of service access settings [14-5](#)  
   Direct Calls [24-1](#)  
   Forwarded Calls [24-1](#)  
   overview [24-1](#)  
 call transfer settings  
   class of service [14-8](#)  
   restriction table [25-1](#)  
   rules [21-7](#)  
   subscriber [17-11](#)  
   subscriber template [13-9](#)  
 circuit-switched integration settings [28-17](#)  
 Cisco Personal Communications Assistant  
   browser settings [8-5](#)  
   specifying a browser language [11-5](#)  
   URL [9-2](#)  
 Cisco Unity Admin account [6-1](#)  
 Cisco Unity Administrator  
   accessing on networked servers [2-3](#)  
   access to [14-5](#)  
   accounts used to access [2-11](#)  
   adding records [3-4](#)  
   creating subscribers [15-16](#)

- finding records [3-4](#)
  - icons [3-3](#)
  - limit to simultaneous access [2-2](#)
  - logging on and exiting [2-1](#)
  - navigation bar [3-1](#)
  - saving data [3-3](#)
  - security concerns [2-1, 2-11](#)
  - specifying a browser language [11-5](#)
  - Cisco Unity Assistant
    - browser settings [8-5](#)
    - settings subscribers can change [9-2](#)
    - specifying a browser language [11-5](#)
    - URL [9-2](#)
  - Cisco Unity Greetings Administrator [21-2](#)
  - Cisco Unity Messaging System account [6-2](#)
  - class of service
    - call transfer settings [14-8](#)
    - deleting [14-2](#)
    - effect on subscribers [14-1](#)
    - enhanced phone security [10-1](#)
    - FaxMail [12-1](#)
    - feature settings [14-9](#)
    - greeting settings [14-9](#)
    - licenses [14-2](#)
    - live reply [14-8](#)
    - maximum message length [14-8](#)
    - messages settings [14-8](#)
    - overview [14-1](#)
    - predefined [14-1](#)
    - profile settings [14-3](#)
    - reassigning subscribers [14-3](#)
    - restriction table settings [14-10, 25-1](#)
    - subscriber settings [14-4](#)
    - system access settings [14-5](#)
  - cleanup interval, logger data files [26-1, 26-2](#)
  - codecs, list of supported [28-4](#)
  - comfort noise [11-6](#)
  - comma delimited files, report format [26-2](#)
  - configuration settings [28-2](#)
  - contacts, system settings [28-5](#)
  - conversation
    - choosing [7-3](#)
    - optional [13-5, 17-7](#)
    - providing ANI information [7-6](#)
    - standard [13-5, 17-7](#)
  - conversation settings
    - specifying for individual subscribers [17-7](#)
    - specifying for subscribers [7-2](#)
    - specifying for subscriber templates [13-5](#)
  - CSV files
    - correcting import errors [15-16](#)
    - optional column headers used by Bulk Import wizard [15-8](#)
    - preparing for Import utility [15-6](#)
    - report format [26-2](#)
- 
- ## D
- data types in Cisco Unity Administrator [3-1](#)
  - defaults
    - call handlers [21-2](#)
    - class of service [14-1](#)
    - configuration settings [28-2](#)
    - Direct Calls call routing table rules [24-1](#)
    - Forwarded Calls call routing table rules [24-1](#)
    - phone and Text to Speech languages [11-3](#)
    - public distribution lists [18-1](#)
    - restriction tables [25-1](#)
    - schedule [28-9](#)
    - subscriber accounts [6-1](#)
    - subscriber template [13-1](#)
  - Delete icon [3-3](#)
  - deleting
    - class of service [14-2](#)
    - distribution list owner [16-1](#)
    - subscriber accounts [16-1](#)
  - diagnostic traces, access to [14-5](#)
  - dialing domains, directory handler searches [22-5](#)

Dialogic codecs [28-4](#)

Direct Calls call routing table settings [24-4](#)

directory assistance [22-1](#)

directory handler

- caller input settings [22-8](#)
- expanding searches with Digital Networking [22-5](#)
- match list options settings [22-6](#)
- overview [22-1](#)
- profile settings [22-3](#)
- search options settings [22-5](#)

distribution lists

- All Subscribers [18-1](#)
- creating [18-2](#)
- creating private lists [17-6](#)
- default lists [18-1](#)
- deleting owner [16-1](#)
- importing from Domino [18-2](#)
- member settings [18-3](#)
- profile settings [18-3](#)
- report [26-5](#)
- subscriber template settings [13-17](#)
- System Event Messages [18-1](#)
- Unaddressed Messages [18-1](#)

Distribution Lists report [26-5](#)

---

## E

EAdministrator account [6-1](#)

end-user documentation [9-1](#)

enhanced phone security

- class of service [10-1](#)
- overview [10-1](#)

Event Log report [26-9](#)

Example Administrator

- account [6-1](#)
- message handling [6-4](#)

Example Interview

- about [6-4](#)
- responsibility for screening [6-4](#)

Example Subscriber account [6-2](#)

exiting the Cisco Unity Administrator [2-3](#)

extensions

- primary vs. alternate [17-25](#)
- remapping [28-20](#)

---

## F

Failed Login report [26-5](#)

fax

- class of service settings [12-1](#)
- delivery and restriction tables [25-1](#)
- integration steps [12-3](#)
- overview [12-1](#)
- sending and receiving via e-mail [12-2](#)
- server integration architecture [12-2](#)

features, Cisco Unity [1-1](#)

feature settings [14-9](#)

Find icon [3-3](#)

Forwarded Calls call routing table settings [24-4](#)

---

## G

G.711 codec [28-4](#)

G.729a codec [28-4](#)

garbled characters when using TTY [11-6](#)

gateways, fax [12-2](#)

glossary [29-1](#)

Goodbye call handler [21-2](#)

GrantUnityAccess utility [2-15](#)

greetings

- call handler settings [21-10](#)
- class of service settings [14-9](#)
- recording [3-5, 7-10](#)
- subscriber settings [17-13](#)
- subscriber template settings [13-11](#)

GUI access, account lockout policy [28-11](#)

## GUI languages

- changing [11-5](#)
- overview [11-1](#)
- system settings [28-6](#)

---

## H

- help desk, orientation [9-5](#)
- holiday settings [28-10](#)

---

## I

- icons, in Cisco Unity Administrator [3-3](#)
- identified subscriber messaging, setting up [28-2](#)
- IIS, configuring for Anonymous Authentication [2-9](#)
- Inherited language setting [11-3](#)
- install account [6-1](#)
- Integrated Windows authentication
  - advantages and disadvantages of [2-5](#)
  - how it works with the Cisco Unity Administrator [2-7](#)
- interview handlers
  - creating [23-1](#)
  - Example Interview [23-1](#)
  - profile settings [23-2](#)
  - questions settings [23-4](#)
- IP integration settings [28-15, 28-16](#)
- ISM (Identified Subscriber Messaging) [28-2](#)

---

## L

- languages
  - changing GUI language [11-5](#)
  - changing phone language [11-3](#)
  - installing Text to Speech [11-1](#)
  - overview [11-1](#)
- legacy phone system integration settings [28-17](#)
- licenses
  - assigning feature access to subscribers [14-9](#)

- counts, for class of service [14-9](#)
- counts, for used and unused [28-11](#)
- language [11-1](#)
- Licensing page, using to view status [28-11](#)
- Text to Speech [14-9](#)
- ViewMail for Lotus Notes [14-9](#)
- Visual Messaging Interface (VMI) [14-9](#)
- live reply [14-8](#)
- locations
  - addressing option settings [27-3](#)
  - profile settings for primary location [27-2](#)
- logger data files [26-1, 26-2](#)

---

## M

- maintenance [4-1](#)
- mapping extensions [28-20](#)
- match list options settings [22-6](#)
- maximum message length, class of service settings [14-8](#)
- Media Master control bar [3-5, 7-10](#)
- member settings, public distribution lists [18-3](#)
- message notifications
  - cascading [17-21](#)
  - chaining [17-21](#)
  - subscriber settings [17-20](#)
  - subscriber template settings [13-17](#)
  - text messages [17-22](#)
- messages
  - addressing in spelling vs. number modes [7-9, 9-3](#)
  - call handler settings [21-13](#)
  - class of service settings [14-8](#)
  - delivery and restriction tables [25-1](#)
  - identified subscriber messaging, setting up [28-2](#)
  - subscriber settings [17-18](#)
  - subscriber template settings [13-15](#)
  - undeliverable [6-3](#)
  - without a specific recipient [6-3](#)
- microphones, using for recording [8-6](#)
- Mu-Law codec [28-4](#)

**N**

- names, recording [3-5, 7-10](#)
- navigation in Cisco Unity Administrator [3-2](#)
- NDRs [6-2, 18-1](#)
- network settings
  - delivery locations profile [27-5](#)
  - overview [27-1](#)
  - primary location addressing option [27-3](#)
  - primary location profile [27-2](#)
- nondelivery receipts [6-2, 18-1](#)
- notifications
  - importing pager information [15-7](#)
  - messages [17-20](#)
- NTLM authentication [2-5](#)

**O**

- one key dialing [20-2](#)
- online Help
  - accessing [3-2](#)
  - Field Help icon [3-3](#)
  - Online Documentation icon [3-3](#)
- Opening Greeting
  - call handler overview [21-2](#)
  - routing to interview handlers [23-1](#)
- Operator call handler
  - overview [21-2](#)
  - responsibility for screening [6-3](#)
- operators, training [9-4](#)
- Optional Conversation 1 [7-3](#)
- orientation
  - operators [9-4](#)
  - subscribers [9-1](#)
  - support desk staff [9-5](#)
- Outcall Billing report [26-7](#)

**P**

- passwords
  - security policy for accessing Cisco Unity by phone [19-1](#)
  - security policy for GUI access [28-11](#)
  - subscriber settings [17-5](#)
  - subscriber template settings [13-4](#)
- PBX integration settings [28-17](#)
- PCA. See Cisco Personal Communications Assistant
- phone access, account lockout policy [19-3](#)
- phone languages
  - changing [11-3](#)
  - overview [11-1](#)
  - system settings [28-5](#)
- phone menu card [9-1](#)
- phone password settings [19-1](#)
- playback speakers for subscribers [8-6](#)
- Port Usage report [26-9](#)
- private lists, creating [17-6](#)
- profile settings
  - call handler [21-5](#)
  - class of service [14-3](#)
  - directory handler [22-3](#)
  - interview handler [23-2](#)
  - primary location [27-2](#)
  - public distribution list [18-3](#)
  - subscriber template [13-2](#)
- prompts, adjusting sound quality [11-6](#)
- public distribution lists
  - All Subscribers [18-1](#)
  - class of service access settings [14-5](#)
  - creating [18-2](#)
  - default lists [18-1](#)
  - deleting owner [16-1](#)
  - Distribution Lists report [26-5](#)
  - importing from Domino [18-2](#)
  - member settings [18-3](#)
  - profile settings [18-3](#)
  - subscriber template settings [13-17](#)

System Event Messages [18-1](#)

Unaddressed Messages [18-1](#)

---

## Q

question settings, interview handler [23-4](#)

quick reference card [9-1](#)

---

## R

recording

enabling warning tone for end of recording [28-19](#)

microphones for subscribers [8-6](#)

system settings [28-4](#)

records

adding [3-4](#)

finding [3-4](#)

saving [3-3](#)

redirecting extensions [28-20](#)

remapping extensions

description [28-20](#)

setup [28-20](#)

syntax and examples [28-22](#)

reports

about data [26-2](#)

access to [14-5, 26-3](#)

Administrative Access Activity report [26-8](#)

Call Handler Traffic report [26-11](#)

Distribution Lists report [26-5](#)

Event Log report [26-9](#)

Failed Login report [26-5](#)

format [26-2](#)

generating [26-2](#)

log-based [26-1, 26-2](#)

Outcall Billing report [26-7](#)

Port Usage report [26-9](#)

snapshot [26-2](#)

Subscriber Message Activity report [26-4](#)

Subscribers report [26-4](#)

System Configuration report [26-10](#)

Transfer Call Billing report [26-6](#)

Unresolved References report [26-11](#)

restarting, Cisco Unity server [A-2](#)

restriction tables

class of service access settings [14-5](#)

class of service settings [14-10](#)

creating [25-3](#)

examples and discussion [25-2](#)

predefined [25-1](#)

settings [25-4](#)

routing rules

adding [22-2, 24-3](#)

providing access to the Cisco Unity Greetings  
Administrator [21-4](#)

RSA SecurID [10-1](#)

Run icon [3-3](#)

---

## S

Save icon [3-3](#)

saving data [3-3](#)

schedules

class of service access settings [14-5](#)

default [28-9](#)

effect on call routing rules [24-2](#)

system settings [28-9](#)

secure logon [10-1](#)

security

account lockout policy for GUI access [28-11](#)

account lockout policy for phone access [19-3](#)

account policy for phone access [19-1](#)

account settings for subscriber template [13-4](#)

best practices for phone passwords [13-4](#)

password policy for GUI access [28-11](#)

password policy for phone access [19-1](#)

subscriber passwords [13-4](#)

shutting down Cisco Unity [A-2](#)

- SIP integration settings [28-16](#)
  - software versions, system settings [28-4](#)
  - speakers, using for playback [8-6](#)
  - SSL [5-1](#)
  - starting Cisco Unity [A-3](#)
  - Status Monitor, access to [14-5](#)
  - Subscriber Message Activity report [26-4](#)
  - subscribers
    - account settings [17-4](#)
    - adding using the Cisco Unity Administrator [15-16](#)
    - alternate extension settings [17-25](#)
    - caller input settings [17-16](#)
    - call transfer settings [17-11](#)
    - class of service [14-1](#)
    - class of service access settings [14-5](#)
    - class of service settings [14-4](#)
    - conversation settings [17-7](#)
    - creating accounts [15-1](#)
    - creating using the Cisco Unity Bulk Import wizard [15-5](#)
    - customizing conversation settings [7-2](#)
    - customizing message playback [7-6](#)
    - default accounts [6-1](#)
    - deleting accounts [16-1](#)
    - greetings settings [17-13](#)
    - identified subscriber messaging, setting up [28-2](#)
    - importing Domino users [15-17](#)
    - maximum greeting length [14-9](#)
    - message notification settings [17-20](#)
    - message settings [17-18](#)
    - password settings [17-5](#)
    - preparing to create [15-2](#)
    - private list settings [17-6](#)
    - profile settings [17-2](#)
    - recording names and greetings [3-5, 7-10](#)
    - secure logons [10-1](#)
    - settings overview [17-1](#)
    - settings subscribers can change [9-2](#)
    - templates [13-1](#)
    - training [9-1](#)
    - unlocking accounts [17-4](#)
  - Subscribers report [26-4](#)
  - subscriber templates
    - account settings [13-4](#)
    - caller input settings [13-13](#)
    - call transfer settings [13-9](#)
    - conversation settings [13-5](#)
    - creating [13-1](#)
    - defaults [13-1](#)
    - distribution list settings [13-17](#)
    - greetings settings [13-11](#)
    - message notification settings [13-17](#)
    - message settings [13-15](#)
    - password settings [13-4](#)
    - profile settings [13-2](#)
    - settings overview [13-1](#)
  - support desk, training [9-5](#)
  - SysCheck utility [26-11](#)
  - system access settings [14-5](#)
  - System Configuration report [26-10](#)
  - System Event Messages public distribution list [18-1](#)
  - system security [10-1](#)
  - system settings
    - configuration settings [28-2](#)
    - contacts [28-5](#)
    - GUI language settings [28-6](#)
    - holiday settings [28-10](#)
    - licensing status [28-11](#)
    - overview [28-1](#)
    - phone language settings [28-5](#)
    - recording settings [28-4](#)
    - schedule settings [28-9](#)
    - software versions [28-4](#)
    - voice port settings [28-14](#)
    - warning tone for end of recording [28-19](#)
- 
- T**
- telephone user interface [7-1, 13-5, 17-7](#)

templates, subscriber

- account settings [13-4](#)
- caller input settings [13-13](#)
- call transfer settings [13-9](#)
- conversation settings [13-5](#)
- creating [13-1](#)
- defaults [13-1](#)
- distribution list settings [13-17](#)
- greetings settings [13-11](#)
- message notification settings [13-17](#)
- message settings [13-15](#)
- password settings [13-4](#)
- profile settings [13-2](#)
- settings overview [13-1](#)

Text to Speech

- e-mail licenses [14-9](#)
- fax settings [12-1](#)
- languages [11-1](#)
- setting default [28-5](#)

toll fraud, preventing [13-4](#)

traditional phone system integration settings [28-17](#)

training

- operators [9-4](#)
- subscribers [9-1](#)
- support desk staff [9-5](#)

Transfer Call Billing report [26-6](#)

transfer settings, call handler [21-7](#)

TRAP [8-7](#)

TTY garbled characters [11-6](#)

TUI [7-1, 13-5, 17-7](#)

---

## U

Unaddressed Messages public distribution list

- overview [18-1](#)
- responsibility for screening [6-3](#)

undeliverable messages [6-3](#)

unidentified callers, defined [24-1](#)

Unresolved References report [26-11](#)

## URL

- Cisco Personal Communications Assistant [9-2](#)
- Cisco Unity Assistant [9-2](#)

user guide [9-1](#)

utilities

- Bulk Edit [15-18, 17-1, 21-2](#)
- GrantUnityAccess [2-15](#)
- SysCheck [26-11](#)

---

## V

ViewMail for Lotus Notes, licenses [14-9](#)

Visual Messaging Interface (VMI)

- licenses [14-9](#)
- message notification [17-22](#)

voice port settings [28-14](#)

---

## W

warning tone for end of recording [28-19](#)

Windows Event Viewer [26-9](#)

Windows NT Challenge/Response authentication [2-5](#)

wizards, Bulk Import [15-5](#)

