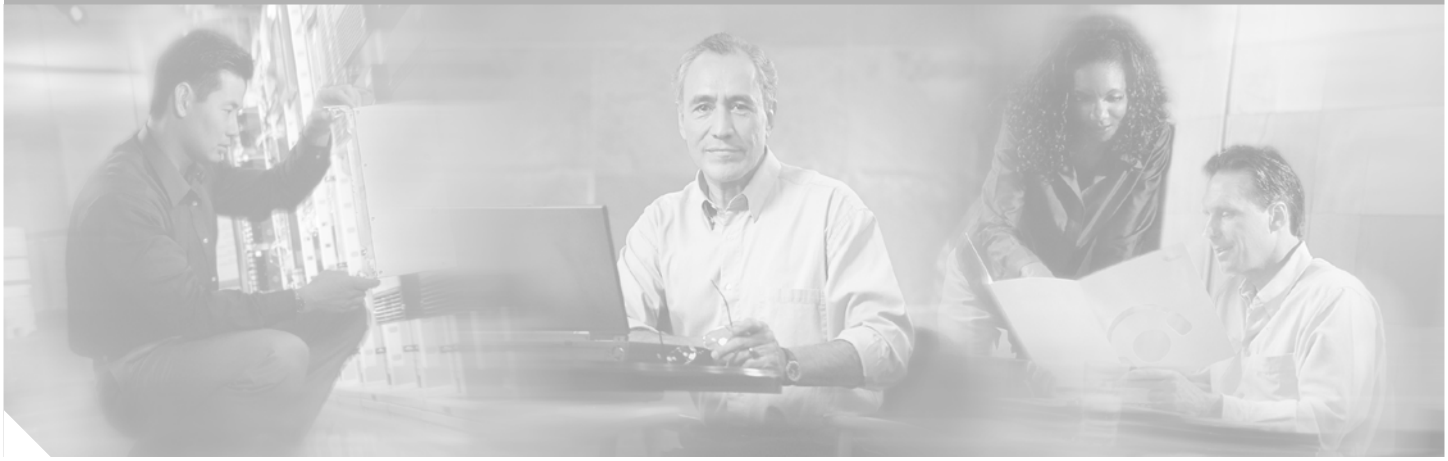

Cisco Unity Connection Troubleshooting Guide

Release 1.x
August 21, 2006

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-11342-01

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

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

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

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

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

Cisco Unity Connection Troubleshooting Guide Release 1.x

CONTENTS

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 9

Preface

This Preface contains the following sections:

Audience and Use

The *Cisco Unity Connection Troubleshooting Guide* contains information on specific problems with Cisco Unity Connection, possible causes of the problems, and procedures to resolve the problems. The guide is written for system administrators who are responsible for maintaining and administering Connection.

Documentation Conventions

Table 1 Cisco Unity Connection Troubleshooting Guide Release 1.x Conventions

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Click **OK**.) • Information that you enter. (Example: Enter **Administrator** in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping <IP address>**.)

Table 1 Cisco Unity Connection Troubleshooting Guide Release 1.x Conventions (continued)

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.)

The Cisco Unity Connection Troubleshooting Guide Release 1.x 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 Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Cisco Unity Connection Documentation Guide*. The document is shipped with Connection and is available at http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations 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.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—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 Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *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/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Diagnostic Traces and Event Logs

In this chapter, you will find information about the diagnostic utilities that enable you to troubleshoot problems and to maintain Cisco Unity Connection, and instructions that will help you in reporting problems to Cisco Technical Assistance Center (Cisco TAC).

See the following sections:

- About the Diagnostic Utilities for Cisco Unity Connection, page 1-1
- Event Log, page 1-2
- Macro Trace Logs in the Cisco Unity Diagnostic Tool (UDT), page 1-2
- Micro Trace Logs in the Cisco Unity Diagnostic Tool (UDT), page 1-4
- Dr. Watson Logs, page 1-9
- Reporting Problems to Cisco TAC, page 1-10

About the Diagnostic Utilities for Cisco Unity Connection

Table 1-1 describes the diagnostic utilities available for Cisco Unity Connection.

Table 1-1 Diagnostic Utilities for Cisco Unity Connection

Utility	Uses
Event log	The Event log should be the first resource you search for information when troubleshooting a problem. The Event log is used by Windows applications to report information events, warnings, and errors. Reviewing the Event log for Connection events provides a good overview of how the system is functioning. For details, see the "Event Log" section on page 1-2.
Macro trace logs in the UDT	In the Cisco Unity Diagnostic tool (UDT), you can enable a preselected group of individual macro trace levels to obtain diagnostic trace output on several Connection components at once. For details, see the "Macro Trace Logs in the Cisco Unity Diagnostic Tool (UDT)" section on page 1-2.

Table 1-1 Diagnostic Utilities for Cisco Unity Connection (continued)

Utility	Uses
Micro trace logs in the UDT	The Cisco Unity Diagnostic tool (UDT) can enable most Connection components to write diagnostic traces to a log. The diagnostic trace output is essential to troubleshooting problems that involve individual components. For details, see the "Micro Trace Logs in the Cisco Unity Diagnostic Tool (UDT)" section on page 1-4.
Dr. Watson logs	The Dr. Watson utility is invoked by Windows 2000 when a serious problem occurs that is not handled by Connection. When invoked, the Dr. Watson utility displays a dialog box that contains an error message (for example, "Dr. Watson encountering an error in the AvCsMgr.exe process"). Dr. Watson errors may occur in other processes as well. For details, see the "Dr. Watson Logs" section on page 1-9.

Event Log

The Event log is the first resource you should search for information when troubleshooting a problem. Cisco Unity Connection components report information events, warnings, and errors in the Event log. Reviewing the Event log for Connection events provides a good overview of how the system is functioning.

Note The raw data within the files in the Event log is stamped with time stamps recorded in GMT (Greenwich mean time) rather than in the local time of the Connection server. The time stamps for the Event log files themselves, however, are in the local time of the Connection server. Using GMT for the time stamps of the raw data provides for an accurate comparison of events when Connection servers are not all in the same time zone. The Connection reports convert the GMT time stamps to local time.

To Obtain an Event Log Trace

Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.

Step 2 In the Tree pane, click **Application**.

Step 3 Search for Connection events.

Note For further instructions on Event Viewer functions, see the Event Viewer Help.

Macro Trace Logs in the Cisco Unity Diagnostic Tool (UDT)

The Cisco Unity Diagnostic tool (UDT) lets you create and view diagnostic trace logs for troubleshooting problems. Diagnostic trace logs of a problem that is occurring can be critical to determining the cause of the problem.

Macro traces in the UDT let you enable preselected groups of micro traces. For details on viewing, interpreting and gathering the micro traces that the macro traces use, see the "Micro Trace Logs in the Cisco Unity Diagnostic Tool (UDT)" section on page 1-4.

Caution Diagnostic traces that are set before a Cisco Unity Connection software upgrade are not preserved and must be reset after the upgrade.

See the following sections:

- Available Macro Traces, page 1-3
- Enabling Macro Traces, page 1-3

Available Macro Traces

Table 1-2 lists the macro traces that are available and what each macro trace analyzes.

Table 1-2 Macro Traces

Macro Trace Name	What the Trace Analyzes
Call Flow Diagnostics	The flow of a call through Connection
Message Objectid Tracking Traces	Message handing; the objects that handle messages from delivery to deletion
Call Control (Miu) Traces	Call control functions
Traces for MWI Problems	Turning message waiting indicators (MWIs) on and off
Traces for Other Notification Problems	Notification and outdial functions
Skinny TSP Traces	The Skinny networking layer; useful only when Connection is integrated with Cisco Unified CallManager
Unity Startup	Connection startup functions
Voice User Interface/Speech Recognition Traces	Voice User Interface (VUI)
Media (Wave) Traces 1 – High-Level	Basic media and WAV file usage
Media (Wave) Traces 2 – Medium-Level	Media and WAV file usage; logs more information than high-level traces
Media (Wave) Traces 3 – Low-Level	Media and WAV file usage; logs detailed information and should be used only when there is significant free hard drive space
Text to Speech (TTS) Traces	The Text to Speech (TTS) feature; also can log traces on other Connection components that interact with TTS

Enabling Macro Traces

Enable the macro trace diagnostics when you are troubleshooting problems with Cisco Unity Connection features. For example, if there are MWI problems, enable the Traces for MWI Problems macro trace. However, keep in mind that running diagnostics can affect system performance and hard drive space.

To Enable Macro Trace Diagnostics

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**. The Cisco Unity Diagnostic Viewer window appears.

Step 2 In the right pane of the Cisco Unity Diagnostic Viewer window, click Configure Macro Traces. The Configure Macro Traces wizard appears.

Step 3 On the Welcome page, click **Next**.

Step 4 On the Configure Macro Traces page, check the check boxes for the applicable traces.

Step 5 Click **Next**.

Step 6 On the Completing page, click **Finish**.

Step 7 In the right pane of the Cisco Unity Diagnostic Viewer window, click **Start New Log Files**.

Step 8 Reproduce the problem.

Note After obtaining the diagnostic trace logs that you want, disable the traces that you enabled.

Micro Trace Logs in the Cisco Unity Diagnostic Tool (UDT)

The Cisco Unity Diagnostic tool (UDT) lets you create and view diagnostic trace logs for troubleshooting problems. Diagnostic trace logs of a problem that is occurring can be critical to determining the cause of the problem.

Micro traces in the UDT let you enable specific Cisco Unity Connection components and trace levels, which makes the trace logs as precise as possible. This is particularly critical when the problem occurs seldom, such as only once a day, as it can be difficult to find the actual occurrence of the problem in a diagnostic trace log.

Caution Diagnostic traces that are set before a Cisco Unity Connection software upgrade are not preserved and must be reset after the upgrade.

See the following sections:

- Available Micro Traces, page 1-4
- Enabling Micro Traces, page 1-7
- Viewing Individual Micro Trace Logs, page 1-8
- How to Interpret Micro Trace Information in the Cisco Unity Diagnostic Tool (UDT), page 1-8
- Gathering Micro Trace Logs into Files, page 1-9

Available Micro Traces

Table 1-3 lists the micro traces that are available and describes what each micro trace analyzes.

Table 1-3 Micro Traces

Micro Trace Name	What the Trace Analyzes
Address Searcher (Address Searcher)	Addressing user-to-user messages
Arbiter (Arbiter)	Conversations, ports, and call routing rules that are used for calls
Bulk Administration Manager (BulkAdministrationManager)	Bulk Administration Manager for creating, updating, and deleting multiple users or system contacts
Certificate Manager (CuCertMgr)	Private secure messaging
Client Data Library (CDL)	
Common Messaging Layer (CML)	
CommServer Manager (AvCsMgr)	Main Cisco Unity Connection process; starting and stopping Connection
ConfigData (ConfigData)	
Conversation Development Environment (CDE)	Conversation engine and conversation events
Database SysAgent Tasks (DataSysAgentTasks)	SysAgent tasks
DbEvent Tasks (DbEvent)	Component notification of database changes
Encryption Library (CuEncrypt)	Encryption (except for messaging) and the encryption audit logs
Failure Conversation (FailureConv)	
GAL: Cache (CuGalCach)	
GAL: Data (CuGalData)	
GAL: Distributed Authoring and Versioning (CuGalDav)	
GAL: SQL (CuGalSql)	
GAL: Test (CuGalTest)	
Gateway (AvCsGateway)	Starting and stopping Cisco Unity Connection; access to AvCsMgr; access to Cisco Unity Connection components
Groupware Access Library (CuGal)	
Licensing (Licensing)	Licensing for per-seat licensed features
Log Manager (AvLogMgr)	Writing diagnostic traces and Event log
Media: Call (MiuCall)	The process between the Miu and conversations
Media: COM Methods (MiuMethods)	Handing of incoming calls; call control; turning messaging waiting indicators (MWIs) on and off; notification and outdial functions; media or WAV file usage
Media: Database (MiuDatabase)	
Media: General (MiuGeneral)	Tracking calls through the telephone user interface (TUI); call control functions; turning message waiting indicators (MWIs) on and off; notification and outdial functions; basic media or WAV file usage

Table 1-3 Micro Traces (continued)

Micro Trace Name	What the Trace Analyzes
Media: Input/Output (MiuIO)	Media or WAV file usage with TAPI (circuit-switched or Cisco Unified CallManager) integrations
Media: Integration (MiuIntegration)	Integrations with circuit-switched phone systems; call information in integrations with circuit-switched phone systems; turning message waiting indicators (MWIs) on and off in integrations with circuit-switched phone systems
Media: SC Bus (MiuSCBus)	Fax engine and fax tone detection
Message Transfer Agent (MTA)	Delivery of voice messages to the message store
Notifier and Notification Devices (Notifier)	Notification of messages and selected events; turning message waiting indicators (MWIs) on and off
Performance Monitor (PerfMonitor)	Performance of system objects that Cisco Unity Connection uses
PHGreeting Conversations (ConvPH Greeting)	Opening greeting and user greetings
PHInterview Conversations (ConvPH Interview)	Interview handler
Phrase Server (PhraseServer)	The prompts that play and the user DTMF input; the logs are written to a file
Phrase Server to Monitor (PhraseServer to Monitor)	The prompts that play and the user DTMF input; the logs are written to the monitor
PHTransfer Conversations (ConvPH Transfer)	Phone transfers
Report Data Library (RDL)	
Resource Loader (Resource Loader)	Using the selected language in the GUI; filling strings with product or message information
Resource Manager (Resource Manager)	Monitoring and providing available resources to the Arbiter as needed
Routing Rules (Routing Rules)	Call routing decisions
Routing Rules Conversation (ConvRoutingRules)	The conversation to which the Arbiter routes calls
Rules Engine (Rules Engine)	
Scheduler (Scheduler)	Currently active Cisco Unity Connection schedule (whether during normal business hours or during nonbusiness hours) or holiday
Server Roles Manager (SRM)	Server Role Manager, which monitors and manages all server roles
Server Status App (CuStatusTray)	The Cisco Unity Connection Server Status utility
Skinny TSP (SkinnyTSP)	*(Circuit-switched or Cisco Unified CallManager phone system integrations)* Media or WAV file usage *(Cisco Unified CallManager SCCP integrations only)* Skinny networking layer

Table 1-3 Micro Traces (continued)

Micro Trace Name	What the Trace Analyzes
Stream Server (StreamServer)	
Subscriber Conversations (Subscriber Conversation)	User activities and usage
System Agent (SysAgent)	System Agent role, which schedules system tasks that the administrator enters (such as resynchronizing MWIs)
Telephone Record and Playback (TRAP)	Telephone Record and Playback (TRAP), which lets clients use the phone as a recording and playback device
Text to Speech (Text to Speech)	Text to Speech feature
UMSS IMAP Server (UMSSIMAPServer)	Access to voice messages by IMAP clients
UMSS Messaging Abstraction Layer (CsMalUmss)	
UMSS SysAgent Tasks (UmssSysAgentTasks)	
Unity Reports Scavenger Service (Scavenger)	Report Data Collector role, which extracts data from log files and periodically cleans up the database
Virtual Queue (VirtualQueue)	Call queuing

Enabling Micro Traces

Enable the micro trace diagnostics when you are troubleshooting problems with specific Cisco Unity Connection components. For example, if there are notification errors in the Event log, enable the Notifier and Notification Devices (Notifier) diagnostics. However, keep in mind that running diagnostics can affect system performance and hard drive space.

To Enable Micro Trace Diagnostics

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**. The Cisco Unity Diagnostic Viewer window appears.

Step 2 In the right pane of the Cisco Unity Diagnostic Viewer window, click **Configure Micro Traces**. The Configure Micro Traces wizard appears.

Step 3 On the Welcome page, click **Next**.

Step 4 On the Configure Micro Traces page, check the check boxes to select the component traces and the trace levels that you want to enable.

Step 5 Click **Next**.

Step 6 On the Completing page, click **Finish**.

Step 7 In the right pane of the Cisco Unity Diagnostic Viewer window, click **Start New Log Files**.

Step 8 Reproduce the problem.

Note After obtaining the diagnostic trace logs that you want, disable the traces that you enabled.

Viewing Individual Micro Trace Logs

Do the following procedure to use the UDT to view individual micro trace logs. For information on interpreting the micro trace information in the UDT, see the "How to Interpret Micro Trace Information in the Cisco Unity Diagnostic Tool (UDT)" section on page 1-8. For instructions on gathering trace logs into files, see the "To Gather Micro Trace Logs into Files" procedure on page 1-9.

To View Individual Micro Trace Logs

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**. The Cisco Unity Diagnostic Viewer window appears.

Step 2 In the left pane of the Cisco Unity Diagnostic Viewer window, expand the **Processes** node.

Step 3 In the left pane, expand the process (or component) that you enabled traces for, and click the log file that you want to view. The log file is formatted and appears in the right pane.

How to Interpret Micro Trace Information in the Cisco Unity Diagnostic Tool (UDT)

When you open a trace log in the UDT, the information is formatted and displayed in columns in the right pane. Table 1-4 lists the information contained in each column of trace logs.

Table 1-4 Information in Trace Logs

Column Name	Information Contained in the Column
#	The line number in the trace log. This number is provided by the UDT and is not contained in the trace log.
Timestamp	The date and time of the trace log.
Source	The source of the trace log text.
Trace No.	The number of the message string that was used from the source identified in the Source column.
Component	The micro trace component that was selected in the Configure Micro Traces wizard.
Level	The trace level that was selected in the Configure Micro Traces wizard.
Trace	The raw data, delimited by commas, from the micro trace.

Gathering Micro Trace Logs into Files

When you are requested to send micro trace logs for examination, you must gather the logs into files. Do the following procedure.

To Gather Micro Trace Logs into Files

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**. The Cisco Unity Diagnostic Viewer window appears.

Step 2 In the right pane of the Cisco Unity Diagnostic Viewer window, click **Gather Log Files**. The Gather Logs wizard appears.

Step 3 On the Welcome page, click **Select Logs**.

Step 4 If you want to change the directory where the files are saved, do the following sub-steps. Otherwise, skip to Step 5.

- **a.** Click **Browse** to select a destination for the files. The Browse for Folder dialog box appears.
- **b.** Click the destination directory where you want the files to be saved, and click **OK**.

Step 5 On the Welcome page, click **Next**.

Step 6 On the Select Logs to Gather page, expand the micro trace processes that you enabled and check the check box for the most recent log for each micro trace.

Step 7 Click **Next**.

Step 8 On the Completing page (after the logs are gathered and formatted), click **View Directory** to open the directory where the files were saved.

Step 9 On the Completing page, click **Finish** to exit the wizard.

Step 10 Close the Cisco Unity Diagnostic Viewer window.

Dr. Watson Logs

Dr. Watson is a program invoked by Windows 2000 when a serious problem occurs that is not handled by Cisco Unity Connection. When Dr. Watson is invoked, a dialog box that contains an error message appears (for example, “Dr. Watson encountering an error in the CuCsMgr.exe process”).

To Obtain a Dr. Watson Log

Step 1 From a command prompt, enter **drwtsn32** and press **Enter**.

Step 2 In the Dr. Watson for Windows dialog box, in the Log File Path field, note the location of the log file.

Step 3 Browse to the Drwtsn32.log file and make a copy of the file in another location.

Step 4 In the Dr. Watson for Windows dialog box, in the Number of Instructions field, enter **50**.

Step 5 In the Number of Errors to Save field, enter the number of errors you want to record. The default is 10.

Step 6 Under Options, confirm that the **Dump All Thread Contexts**, **Append to Existing Log File**, **Visual Notification**, and **Create Crash Dump File** check boxes are checked.

Step 7 Click **OK** to close the dialog box.

Step 8 Reproduce the problem.

Step 9 Browse to the **Drwtsn32.log** file and make a copy of the file in another location.

Reporting Problems to Cisco TAC

When you report a problem to the Cisco Technical Assistance Center (Cisco TAC), you will be asked to provide information about your system and about the problem. This section provides procedures for gathering the system information and problem descriptions that may be requested.

System Information

Have the following system information ready when you call:

- The results from running the Gather Unity System Info utility. See the "To Collect the Cisco Unity Connection System Information" procedure on page 1-10.
- Number and type of voice ports installed.
- Number of users in the Cisco Unity Connection database.
- Number, type, and speed of processors.
- Memory and pagefile size.
- Hard disk size and free space available.
- Phone system integration, including the manufacturer, model, and version (if applicable).
- Other telephony software or hardware installed, such as fax.
- Microsoft Windows 2003 service packs installed.
- Approximate normal Connection server CPU utilization. (For example, does the Windows task manager often show 100 percent CPU utilization, or is it usually less than 80 percent?)

To Collect the Cisco Unity Connection System Information

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Gather Unity System Info**.

Step 2 In the Gather Unity System Info window, note the system information that is displayed.

Problem Description

Be prepared to give a complete description of the problem, including:

- Symptoms such as lost ports, Event log errors, or Dr. Watson errors.
- Problem frequency under normal load conditions (for example, every call, once per hour, or once only).
- Problem frequency when specific attempts are made to reproduce it.
- Detailed sequence of steps to reproduce the problem.

- Date and time of last known occurrence of the problem.
- Which digits were entered by the caller (for example, menu selections or user extensions, or the extension of the caller or called port), if known.
- Which port(s) were affected by the problem, if known.
- Applicable logs and traces. For information on how to obtain log and trace files, see the preceding sections of this chapter.

Utilities

This chapter contains the following sections:

- Cisco Security Agent for Cisco Unity, page 2-1
- Cisco Unity Connection Disaster Recovery Tools (DiRT), page 2-1
- Cisco Unity Connection Server Status Utility, page 2-2
- Cisco Unity Connection Bulk Administration Manager, page 2-2
- Port Status Monitor, page 2-3
- Port Usage Analyzer, page 2-4
- Tools Depot, page 2-4
- Call Viewer, page 2-5

Cisco Security Agent for Cisco Unity

Cisco Security Agent for Cisco Unity is designed to not interfere with normal operations of Cisco Unity Connection. The Cisco Unity Connection Setup program and Cisco Unity Connection Server Updates wizard are both designed to disable Cisco Security Agent for Cisco Unity prior to installing files and to re-enable Cisco Security Agent for Cisco Unity after installation is compete.

See the "Cisco Unity Connection Disaster Recovery Tools (DiRT)" section on page 2-1 for information about a problem when you are running Cisco Security Agent for Cisco Unity version 2.0(2) and using Disaster Recovery tools.

Cisco Unity Connection Disaster Recovery Tools (DiRT)

The Disaster Recovery Backup tool may fail with errors when Cisco Security Agent for Cisco Unity version 2.0(2) is running. Version 2.0(2) prevents the MS SQL service from writing some of the database backup files.

If you are using Cisco Security Agent for Cisco Unity version 2.0(2), uninstall it and install Cisco Security Agent for Cisco Unity version 2.0(3) or later. For more information, see the Cisco Security Agent for Cisco Unity release notes at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

Cisco Unity Connection Server Status Utility

The Cisco Unity Connection Server Status utility lets you monitor the status of the Connection server, manage server roles, and monitor voice messaging ports through two interfaces:

- The Server Status window provides the Server Status, Server Roles, Ports, and Help tabs.
- In the status area of the task bar, the Cisco Unity Connection icon provides server status information and a shortcut menu.

For information on using the Server Status utility, see the Help tab in the Server Status window.

Restarting the Cisco Unity Connection Server Status Utility

You can do the following procedure to restart the Cisco Unity Connection Server Status utility when it is not running.

To Restart the Cisco Unity Connection Server Status Utility

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Connection Server Status**.

Note When the Server Status utility window is minimized (the Server Status utility icon still appears in the status area of the task bar), you can restore the window by right-clicking the Server Status utility icon and clicking Restore.

Exiting the Cisco Unity Connection Server Status Utility

Exiting the Cisco Unity Connection Server Status utility does not stop the Connection server or affect calls that are in progress. Only the Server Status utility stops running, and the icon on the taskbar is removed.

To Exit the Cisco Unity Connection Server Status Utility

Step 1 In the status area of the task bar, right-click the Server Status utility icon and click **Exit**.

Cisco Unity Connection Bulk Administration Manager

Troubleshooting Bulk Administration Manager Failures

When you run Bulk Administration Manager to create, update, or delete users or contacts, it copies each record that it cannot process to a failed objects report file, along with the reason that the record was not processed correctly.

For example, in the following CSV file, the first record includes an invalid entry for the Country field, and the second record specifies a template that is not a voice mail user template:

```
Alias, City, PostalCode, State, Country, TemplateAlias
Jsmith, Beverly Hills, 90210, Ca., United States, VoiceMailUserTemplate
BRobertson, Seattle, 98121, WA, US, AdminUserTemplate
```

When this file is used to create users with voice mail, the following failed objects file is produced:

```
FailureReason, alias, city, postalcode, state, country, templatealias
United States is invalid for column Country|, Jsmith, Beverly Hills, 90210, Ca., United
States, VoiceMailUserTemplate
Object not found or is not a template:  Parameter = [@TemplateObjectId], Table =
[vw_SubscriberTemplate], Column = [Alias,ObjectId]|, BRobertson, Seattle, 98121, WA, US,
AdminUserTemplate
```

The FailureReason column—which provides information about the invalid data—is added before the first column.

To correct errors, do the following procedure to modify the failed objects file, rename it, and use it as the input file when you re-run Bulk Administration Manager.

Note that depending on the type of problem with the data in the CSV file, for each problem record, Bulk Administration Manager may report multiple errors or only the first error encountered. Therefore, after you correct errors, Bulk Administration Manager may detect additional errors in the same record when the data is processed again. Thus, you may need to repeat the correction process—running the tool and correcting an error—several times to find and correct all errors.

To Correct Errors in Creating, Updating, or Deleting Users or Contacts by Using the Failed Objects File

Step 1 Go to the directory location of the failed objects file that you specified when you ran Bulk Administration Manager. (If you are running the wizard, the default location and file name is <Input file directory>\<Input file name>.failed.csv.)

Step 2 Open the file and correct all problems with the data, as indicated by the information in the FailureReason column for each record.

Step 3 Remove the FailureReason column or change the heading to “junk.”

Step 4 When you have finished modifying the data, save the file as a CSV file with a new name.

Step 5 Run Bulk Administration Manager again with the CSV file that you saved in Step 4 as the input file.

Note that each time that you run Bulk Administration Manager, the failed objects file is overwritten (unless you specify a new name for the file each time you run the tool).

Step 6 Repeat this procedure until all records are processed without error.

Port Status Monitor

The Port Status Monitor lets you to monitor Cisco Unity Connection voice port activity in real time. Do the following procedure to start the Port Status Monitor.

To Start the Port Status Monitor

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Port Status Monitor**.

For information on using the utility, see Port Status Monitor Help.

Port Usage Analyzer

The Port Usage Analyzer is a suite of four reports that can provide comprehensive information about the call-traffic loads experienced by the Cisco Unity Connection server. Do the following procedure to start the Port Usage Analyzer.

To Access the Port Usage Analyzer

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Port Usage Analyzer**.

For information on using the utility, see Port Usage Analyzer Help.

Tools Depot

The Cisco Unity Tools Depot is a collection of utilities that perform a variety of administration, audio management, diagnostic, reporting, and phone system integration functions.

To Access the Tools Depot

Step 1 Double-click the Cisco Unity Tools Depot icon on the Cisco Unity Connection server desktop.

or

On the Windows Start menu, click **All Programs > Cisco Unity > Cisco Unity Tools Depot**.

The left pane of the Tools Depot lists all of the available utilities by category.

Step 2 To run a utility, double-click the name in the left pane.

To display the Help for a utility, click the name in the left pane.

Most of the utilities in the Tools Depot are also available on the Cisco Unity Tools website (http://ciscounitytools.com), where updates to utilities are frequently posted between Cisco Unity Connection releases. If the Connection server is connected to the Internet and you run a Tools Depot utility that is available on the Cisco Unity Tools website, the utility automatically checks to see whether an updated version is available. If the Connection server is not connected to the Internet, we recommend that you check the Cisco Unity Tools website to determine whether a later version of the utility is available.

Some utilities work only with selected versions of Connection. If a utility does not appear in the Tools Depot, it does not work with the version of Connection currently running.

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

Call Viewer

For each call that the phone system integration sends to Cisco Unity Connection, the Call Viewer displays one line of information. This information can be helpful when troubleshooting problems with the phone system integration, as well as testing call routing rules. (See Table 2-1 for details on the information displayed.)

The Call Viewer displays integration information for inbound calls only. To see call information for outbound calls, use the Port Status Monitor. For instructions on starting the Port Status Monitor, see the "Port Status Monitor" section on page 2-3.

To Start the Call Viewer

Step 1 On the Cisco Unity Connection server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane of the Tools Depot window, expand the **Switch Integration Tools** node.

Step 3 Double-click **Call Viewer**.

The Call Viewer window displays call information that the phone system integration provides to Cisco Unity Connection for inbound calls.

Table 2-1 lists the information that the Call Viewer displays.

Table 2-1 Call Viewer Information

Column Head	Information Displayed
Call #	The number of the call as it was presented to Cisco Unity Connection.
Time	The time that the call was presented to Cisco Unity Connection.
Origin	• Internal—The call originated from an extension on the phone system. • External—The call originated from a phone that is not an extension on the phone system. • Unknown—The source of the call is not known.
Reason	• Direct—The caller dialed or was transferred to the Cisco Unity Connection pilot number. • Forward (Ring no answer)—The call was forwarded to Connection because the extension the caller dialed was not answered. • Forward (Busy)—The call was forwarded to Connection because the extension the caller dialed was busy. • Forward (All)—The call was forwarded to Connection because the extension was set to forward all calls.
Trunk ID	*(If provided by the phone system)* The number of the trunk that the call arrived on.

Table 2-1 Call Viewer Information (continued)

Column Head	Information Displayed
Port ID	The display name of the voice messaging port as it appears in Cisco Unity Connection Administration on the Search Ports page in Telephony Integrations. The Port ID is not the extension number of the voice messaging port.
Dialed Number	*(If provided by the phone system)* The extension number that the caller dialed.
Calling Number	*(If provided by the phone system)* The extension number of the phone on which the call was dialed.
Forwarding Station	*(If provided by the phone system)* When the call is forwarded to Cisco Unity Connection, the extension number of the phone that the call was forwarded from.

Reports

This chapter contains the following sections:

- Available Reports, page 3-1
- Troubleshooting Report Generation, page 3-3

Available Reports

Table 3-1 lists the available Cisco Unity Connection reports, and the data that each report provides.

Table 3-1 Cisco Unity Connection Reports

Report Name	Description of Output
Call Handler Traffic	Output includes the following information for each call handler, in rows for each hour of a day: • Total number of calls • Number of times each touchtone key was pressed • Extension • Number of times the after greeting action occurred • Number of times the caller hung up
Distribution Lists	Output includes the following information: • Alias and display name of the list • Date and time the list was created • Date and time of the creation of the distribution list is given in Greenwich mean time. • A count of the number of users included in the list • If the Include List Members check box is checked, a listing of the alias of each user who is a member of the list

Table 3-1 Cisco Unity Connection Reports (continued)

Report Name	Description of Output
Outcall Billing Detail	Output includes the following information, arranged by day and by the extension of the user who placed the call: • Name, extension, and billing ID • Date and time the call was placed • The phone number called • The result of the call (connected, ring-no-answer (RNA), busy, or unknown) • The duration of the call in seconds
Outcall Billing Summary	Output is arranged by date and according to the name, extension, and billing ID of the user who placed the call, and is a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span.
System Configuration	Output includes detailed information about all aspects of the configuration of the Cisco Unity Connection system.
Transfer Call Billing	Output includes the following information for each call: • Name, extension, and billing ID of the user • Date and time that the call occurred • The phone number dialed • The result of the transfer (connected, ring-no-answer (RNA), busy, or unknown)
Phone Interface Failed Logon	Output includes the following information for every failed attempt to log on to Cisco Unity Connection by phone: • User name, alias, caller ID, and extension of the user who failed to log on • Date and time that the failed logon occurred • Whether the maximum number of failed logons has been reached for the user
Unused Voice Mail Accounts	Output includes user alias and display name, and the date and time that the user account was created. Date and time of the creation of the user account is given in Greenwich mean time.
User Lockout	Output includes user alias, the number of failed logon attempts for the user, credential type, and the date and time that the account was locked. Date and time of the lockout of the user account is given in Greenwich mean time.

Table 3-1 Cisco Unity Connection Reports (continued)

Report Name	Description of Output
User Message Activity	Output includes the following information about messages sent and received, per user: • Name, extension, and class of service • Date and time for each message • Information on the source of each message • Action completed (for example, user logged in, new message, message saved, MWI On requested, and so on) • Information on the number of new messages received for a user, and on the message sender • Dial out number and results
Users	Output includes the following information for each user: • Last name, first name, and alias • Information that identifies the Cisco Unity Connection server associated with the user • Billing ID, class of service, and extension • Whether the account is locked • Whether the user has enabled personal call transfer rules

Troubleshooting Report Generation

The time necessary for a report to complete varies, depending on the size of the database and on how busy the system is.

Ideally, database and log file sizes should be less than 2 GB, and large reports should be run at times when they have the least affect on the system.

If the wait time for the report seems excessive, do one or more of the following:

- Cancel the report and request it again at a time when the system is not as busy. Do the "To Cancel a Report" procedure on page 3-4.
- Try running the report for a smaller data set. For example, decrease the date range for the report.
- Check the sizes of the database and log files. By default, the log .ldf files are located in the E:/UC_DatabaseLogs directory and the database .mdf files are in the F:/UC_Databases directory on the server.
- Turn on diagnostic traces for a report, then run a small report. Do the "To Turn on Diagnostic Traces for Reports" procedure on page 3-4.
- Check the event log for any SQL Server errors or web service errors. (To view the event log, on the Windows Start menu, click Programs >Administration Tools >Event Viewer.)
- Try running the report, selecting a different form of output. For example, if you tried to generate the report in PDF format, try to generate it as a web page.

If the report still is not produced, and you are unable to determine the cause of the problem from the diagnostic logs, or if the database or log files are too large, contact Cisco TAC.

To Cancel a Report

⚠ **Caution** Cancelling a report involves stopping SQL Server and Cisco Unity Connection; do not do this procedure when these services must be running.

Step 1 Stop the browser, or log out of Cisco Unity Connection Administration.

Step 2 Stop Cisco Unity Connection by right-clicking the Connection Server Status icon in the status tray, and clicking **Stop > Cisco Unity Connection**.

Step 3 Stop the SQL Server task by using Task Manager.

Step 4 Restart the SQLAgent$CISCOUNITY service by using the Services console.

Step 5 Restart Connection by right-clicking the Connection Server Status icon in the status tray, and clicking **Start > Cisco Unity Connection**.

To Turn on Diagnostic Traces for Reports

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**.

Step 2 In the Cisco Unity Diagnostic Tasks pane, click **Configure Micro Traces**.

Step 3 On the Configure Micro Traces Wizard Welcome screen, click **Next**.

Step 4 Check the **Report Data Library (RDL)** check box.

Step 5 Click **Next**.

Step 6 Click **Finish**.

Step 7 Generate a report.

Step 8 To view the log files, in the left pane of the Cisco Unity Diagnostics screen, expand **Cisco Unity Diagnostic Tool >Processes > CuCsMgr**, and then click the current log file.

The selected log file is formatted and displayed in the right pane.

Step 9 To save a copy of the log file, right-click the file in the left pane, click **All Tasks > Gather Log Files**, and then follow the prompts in the Gather Logs Wizard.

Step 10 To turn off the traces set in Step 4, right-click **Cisco Unity Diagnostic Tool**, and click **All Tasks > Reset to Default Traces**.

Phone System Integration

This chapter contains the following sections:

Preparations for Troubleshooting the Phone System

Problems with external and internal calls, message notification calls, and message waiting indicators (MWIs) can be caused by the phone system, by Cisco Unity Connection, or by both, and are therefore difficult to diagnose. Several of the procedures for resolving problems use the single-line test, in which the phone lines connected to Connection are tested one at a time.

Most phone systems provide documentation on the codes that perform transfers, recalls, and other call progress functions. Have the phone system documentation available while doing the procedure steps in this section.

Setting Up For a Diagnostic Test

To do diagnostic tests, you need two test extensions. Phone 1 is assigned to a test user. Phone 2 is set up only in the phone system and does not need to have a Cisco Unity Connection user assigned. The two extensions must be in the same calling search space as the pilot number for Connection.

To Set Up the Test Configuration

Step 1 Set up two test extensions (Phone 1 and Phone 2) on the same phone system that Cisco Unity Connection is connected to.

Step 2 Set Phone 1 to forward calls to the Connection pilot number when calls are not answered or when the phone is busy.

Step 3 To create a test user for testing, in Cisco Unity Connection Administration, expand **Users**, then click **Users**.

Step 4 On the Search Users page, on the User menu, click **New User**.

Step 5 On the New User page, enter the following settings.

Table 4-1 Settings for the New User Page

Field	Setting
User Type	User with Voice Mailbox
Based on Template	<the applicable user template>
Alias	testuser
First Name	Test
Last Name	User
Display Name	Test User
Extension	<the extension of Phone 1>

Step 6 Click **Save**.

Step 7 On the Edit User Basics page, in the Voice Name field, record a voice name for the test user.

Step 8 In the Phone System field, confirm that the phone system selected is the phone system that Phone 1 is connected to.

Step 9 Uncheck the **Set for Self-Enrollment at Next Login** check box.

Step 10 Click **Save**.

Step 11 On the Edit menu, click **Message Waiting Indicators**.

Step 12 On the Message Waiting Indicators page, click the message waiting indictor. If no message waiting indication is in the table, click **Add New**.

Step 13 On the Edit Message Waiting Indicator page, enter the following settings.

Table 4-2 Settings for the Edit Message Waiting Indicator Page

Field	Setting
Enabled	Check this check box to enable MWIs for the test user.
Display Name	Accept the default or enter a different name.
Inherit User’s Extension	Check this check box to enable MWIs on Phone 1.

Step 14 Click **Save**.

Step 15 On the Transfer Options page, click the active option.

Step 16 On the Edit Transfer Options page, under Transfer Action, click the **Extension** option and enter the extension of Phone 1.

Step 17 In the Transfer Type field, click **Release to Switch**.

Step 18 Click **Save**.

Accessing Cisco Unity Telephony Integration Manager

Cisco Unity Connection does not use the Cisco Unity Telephony Integration Manager (UTIM) tool. The same functionality is located under Telephony Integrations in Cisco Unity Connection Administration. You can add and edit integrations there, as well as set port capabilities.

Running the Check Telephony Configuration Test

If the following conditions exist, test the telephony configuration in Cisco Unity Connection Administration:

- Calls to Cisco Unity Connection are failing
- The application event log indicates problems with the Cisco Unity-CM TSP
- Ports are failing to register

To run the Check Telephony Configuration test, click the link in the Related Links box in the upper right corner of any Telephony Integrations page in Connection Administration.

Troubleshooting Integrations with Cisco Unified CallManager

See the following sections:

- Viewing or Editing the IP Address of a Cisco Unified CallManager Server, page 4-3
- Troubleshooting Problems That Occur When Cisco Unity Connection Is Configured for Cisco Unified CallManager Authentication and Encryption, page 4-4
- Determining the Correct Port Group Template, page 4-7

Viewing or Editing the IP Address of a Cisco Unified CallManager Server

Do the following procedure to view or change the IP address or other settings of a Cisco Unified CallManager server.

To Change Cisco Unified CallManager Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for which you want to change Cisco Unified CallManager server settings.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under Cisco Unified CallManager Servers, change the applicable settings and click **Save**.

Step 5 In the Windows taskbar, right-click the Cisco Unity Connection icon and click **Restart > Voice Processing Server Role**.

Step 6 When prompted to confirm stopping the Voice Processing server role, click **Yes**.

Troubleshooting Problems That Occur When Cisco Unity Connection Is Configured for Cisco Unified CallManager Authentication and Encryption

When Cisco Unity Connection is integrated by SCCP with a Cisco Unified CallManager phone system, you have the option of setting up Cisco Unified CallManager authentication and encryption. If the IP address for the TFTP server has not been entered correctly, or if the root certificate for the Connection server has not been copied to the Cisco Unified CallManager server, problems can occur.

See the following sections:

- Cisco Unity Connection Will Not Start, page 4-4
- Cisco Unity Connection Does Not Answer Calls, page 4-5

Note For information on integrating Cisco Unity Connection with Cisco Unified CallManager, see the applicable Cisco Unified CallManager integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Cisco Unity Connection Will Not Start

If the following conditions exist, you will need to confirm that the IP address for the TFTP server has been entered correctly:

- Connection ports are set properly for authentication or encryption.
- The port settings match on Connection and Cisco Unified CallManager.
- On restart there are errors in the application event log.
- Connection will not start.

If the IP address for the TFTP server has not been entered, or was entered incorrectly, do the following "To Add or Edit the IP Address for a TFTP Server" procedure.

To Add or Edit the IP Address for a TFTP Server

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

Step 2 On the Search Port Groups page, click the display name of the port group for your Cisco Unified CallManager integration.

Step 3 On the Port Group Basics page, on the Edit menu, click **Servers**.

Step 4 On the Edit Servers page, under TFTP Servers, click **Add**.

Step 5 Enter the IP address for the TFTP server and click **Save**.

Step 6 In the Windows taskbar, right-click the Cisco Unity Connection icon and click **Restart > Voice Processing Server Role**.

Step 7 When prompted to confirm stopping the Voice Processing server role, click **Yes**.

Cisco Unity Connection Does Not Answer Calls

If the following conditions exist, confirm that the root certificate for the Connection server has been copied to the Cisco Unified CallManager server:

- The Connection ports are set properly for authentication or encryption.
- The port settings match on Connection and Cisco Unified CallManager.
- On restart there are errors in the application event log.
- Connection does not answer calls.

If the root certificate for the Connection server has not been copied to the Cisco Unified CallManager server, do the applicable procedure:

- To Copy the Root Certificate for Cisco Unified CallManager 4.x, page 4-5
- To Copy the Root Certificate for Cisco Unified CallManager 5.0, page 4-5

To Copy the Root Certificate for Cisco Unified CallManager 4.x

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the name of the Cisco Unified CallManager phone system for which you want to enable authentication and encryption of the Connection voice messaging ports.

Step 3 On the Phone System Basics page, on the Edit menu, click **Root Certificate**.

Step 4 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and click **Save Target As**.

Step 5 In the Save As dialog box, browse to the location on the Connection server where you want to save the Cisco Unity Connection root certificate as a file.

Step 6 In the File Name field, confirm that the extension is .0 (rather than .htm), and click **Save**.

Caution The certificate must be saved as a file with the extension .0 (rather than .htm) or Cisco Unified CallManager will not recognize the certificate.

Step 7 In the Download Complete dialog box, click **Close**.

Step 8 Copy the Cisco Unity Connection root certificate file to the C:\Program Files\Cisco\Certificates directory on all Cisco Unified CallManager servers in this Cisco Unified CallManager phone system integration.

Step 9 In Cisco Unity Connection Administration, in the Related Links list, click **Check Telephony Configuration** and click **Go** to confirm the connection to the Cisco Unified CallManager servers.

To Copy the Root Certificate for Cisco Unified CallManager 5.0

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.

Step 2 On the Search Phone Systems page, click the name of the Cisco Unified CallManager phone system for which you want to enable authentication and encryption of the Connection voice messaging ports.

Step 3 On the Phone System Basics page, on the Edit menu, click **Root Certificate**.

Step 4 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and click **Save Target As**.

Step 5 In the Save As dialog box, browse to the location on the Connection server where you want to save the Cisco Unity Connection root certificate as a file.

Step 6 In the File Name field, confirm that the extension is .pem (rather than .htm), and click **Save**.

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

When Cisco Unity Connection is integrated with both Cisco Unified CallManager 4.x and Cisco Unified CallManager 5.x servers, you must copy the .pem file to the Cisco Unified CallManager 5.x server and the .0 file to the Cisco Unified CallManager 4.x server. Otherwise, authentication and encryption will not function correctly.

Step 7 In the Download Complete dialog box, click **Close**.

Step 8 Copy the Cisco Unity Connection root certificate to all Cisco Unified CallManager servers in this Cisco Unified CallManager phone system integration by doing the following substeps.

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

a. On the Cisco Unified CallManager server, in Cisco Unified CallManager Platform Administration, on the Security menu, click **Certificate Management > Upload Certificate/CTL**.

b. On the Cisco IPT Platform Administration page, click **Upload Trust Certificate** and **CallManager - Trust**, then click **OK**.

c. Browse to the Cisco Unity Connection root certificate that you saved in Step 6.

d. Follow the on-screen instructions.

e. Repeat Step 8a. through Step 8d. on all remaining Cisco Unified CallManager servers in the cluster.

f. In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **Go** to confirm the connection to the Cisco Unified CallManager servers.

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

g. In the Task Results window, click **Close**.

Step 9 If prompted, restart the Cisco Unity Connection software.

Determining the Correct Port Group Template

When adding a phone system integration for Cisco Unified CallManager, there are two options for the Port Group Template: SCCP - Skinny Client Control Protocol or SIP - Session Initiation Protocol. The SIP protocol is valid only with Cisco Unified CallManager 5.0(1) and later.

To integrate Cisco Unity Connection with a Cisco SIP Proxy Server, select the SIP Proxy Server option rather than the Cisco Unified CallManager option in the Model list on the Select Phone System Model page of the Phone System Integration wizard.

Installation and Licensing

This chapter contains the following sections:

- Installation or Upgrade from Downloaded Software Fails, page 5-1
- A Drive Is Filling Up, page 5-1
- Removing a License File, page 5-4
- Determining Licensing Status, page 5-4

Installation or Upgrade from Downloaded Software Fails

If you downloaded Cisco Unity Connection from the Cisco website and burned a disc without having the disc-burning application verify the burned disc, a Connection installation or upgrade may fail with any of a variety of errors because of errors on the burned disc. We recommend the following:

- When you download the software, make note of the MD5 value, and use a checksum generator to verify that the MD5 checksum of the downloaded .iso file matches the checksum that is listed on Cisco.com. Free checksum tools are available on the Internet.
- When you burn a disc of the downloaded software, choose the option to verify the contents of the burned disc, which compares the contents of the disc with the contents of the downloaded .iso file.

A Drive Is Filling Up

A drive may fill up for two different reasons. See the applicable section:

- Connection Was Uninstalled and Reinstalled, page 5-1
- G: Drive Is Missing, page 5-2

Connection Was Uninstalled and Reinstalled

When you uninstall Cisco Unity Connection, the Connection uninstaller does not remove Connection database and log directories on the E: and F: drives. If you then reinstall Connection without reinstalling the operating system by using the Cisco Platform Configuration disc, Connection Setup cannot move databases and logs from the installation drive to drives E: and F: because the directories in the target location already exist.

Because the database on the installation drive is in use, moving it is a complex and error-prone process. If you encounter this problem, we recommend that you resolve it by doing the following tasks:

1. Back up the Cisco Unity Connection data by using the Connection Disaster Recovery Backup tool (DiRT). The latest version of the Disaster Recovery Backup tool (and the Disaster Recovery Restore tool, which you will need in task 3.) is available at http://ciscounitytools.com/App_CUC_DisasterRecoveryTool.htm. (Both tools are also in Cisco Unity Tools Depot.) For information on using Disaster Recovery tools, see the DiRT Help.
2. Reinstall and reconfigure all software on the Connection server. In the *Cisco Unity Connection Installation Guide, Release 1.x*, in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System" chapter, do Task 2, and Task 4 through Task 7.

   Caution When you reinstall and reconfigure Windows, you must give the server the same name that it had before the reinstall, or any SSL certificates that you installed on the Connection server will be invalid.

   You can skip the following sections in the "Setting Up and Configuring the Server, and Obtaining License Files" chapter:

   – "Installing a Memory Upgrade (Selected Servers Only)"

   – "Setting Up the Server"

   – "Configuring a Dual NIC"

   – "Obtaining Cisco Unity Connection License Files (Connection Server Only)"

   The *Cisco Unity Connection Installation Guide, Release 1.x* is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.
3. Restore the data that you backed up in Task 1. by using the Connection Disaster Recovery Restore tool.

G: Drive Is Missing

If you installed Windows while a device was plugged in to a USB port on the Cisco Unity Connection server, the device may have been interpreted as a storage device and may have been assigned drive letter G. (The device need not be a removable storage device for this problem to occur.) As a result, data that would have been moved from the installation drive during Connection setup (including the directory for message files, and Connection languages) remains on that drive, and the drive quickly fills up.

To Determine Whether Drive G: Was Assigned to a USB Device

Step 1 On the Cisco Unity Connection server, open Windows Explorer.

Step 2 On the View menu, click **Details**.

Step 3 In the left frame, click **My Computer**.

Step 4 In the right frame, confirm that the device type for drives C:, D:, E:, F:, and G: is Local Disk.

Step 5 If the device type for any of the drives is not Local Disk, do the following "To Resolve a Problem with a Missing Drive G:" procedure.

To Resolve a Problem with a Missing Drive G:

Step 1 Back up the Cisco Unity Connection data by using the Connection Disaster Recovery Backup tool (DiRT).

Note The latest version of the Disaster Recovery Backup tool (and the Disaster Recovery Restore tool) is available at http://ciscounitytools.com/App_CUC_DisasterRecoveryTool.htm. (Both tools are also in Cisco Unity Tools Depot.) For information on using the Disaster Recovery tools, see the DiRT Help.

Step 2 Delete the existing RAID configuration by doing the applicable sub-steps, depending on your server.

Caution Deleting the RAID configuration deletes all applications and all data on the Connection server.

If the Connection server was manufactured by Hewlett Packard:

a. Start the server, and, when prompted to press Ctrl-A to start the Adaptec RAID Configuration Utility, press **Ctrl-A**.

b. Select Array Configuration Utility, and press **Enter**.

c. Select Manage Arrays, and press **Enter**.

d. In the list of RAID arrays, select the first RAID array, and press **Del** to delete it.

e. Repeat Step d. until you have deleted all RAID arrays.

f. Exit the utility.

g. If you are prompted to save changes, choose the option to save.

If the Connection server was manufactured by IBM:

a. Start the server and, at system POST, press the applicable keys to start IBM ServeRAID Mini Configuration. On most IBM servers, this is **Ctrl-I**.

b. On the IBM ServeRAID Mini Configuration Main Menu, select **Advanced Functions**, and press **Enter**.

c. On the IBM ServeRAID Mini Configuration Advanced Functions Menu, select **Restore to Factory-Default Settings**, and press **Enter**.

d. Follow the on-screen prompts.

Step 3 Reinstall and reconfigure all software on the Connection server. In the *Cisco Unity Connection Installation Guide, Release 1.x*, in the “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” chapter, do Task 2, and Task 4 through Task 7.

Caution When you reinstall and reconfigure Windows, you must give the server the same name that it had before the reinstall, or any SSL certificates that you installed on the Connection server will be invalid.

You can skip the following sections in the “Setting Up and Configuring the Server, and Obtaining License Files” chapter:

- “Installing a Memory Upgrade (Selected Servers Only)”

- "Setting Up the Server"
- "Configuring a Dual NIC"
- "Obtaining Cisco Unity Connection License Files (Connection Server Only)"

Note The *Cisco Unity Connection Installation Guide, Release 1.x* is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Step 4 Restore the data that you backed up in Step 1 by using the Connection Disaster Recovery Restore tool.

Removing a License File

Although you can add multiple license files by using the Cisco Unity Connection Configuration Assistant, you cannot use it to remove license files.

To remove license files, in Cisco Unity Connection Administration, expand System Settings > Licenses. On the Licenses page, uncheck the check box(es) for the license file(s) that you want to remove and click Delete Selected.

License files are not physically removed from the system, but they are no longer installed. To remove a license file from the list of files on the Licenses page, delete the file from the Program Files\Cisco Systems\Cisco Unity Connection\Licenses directory.

Determining Licensing Status

To determine the licensing status of Cisco Unity Connection, in Cisco Unity Connection Administration, expand System Settings > Licenses. On the Licenses page, click the applicable report link in the upper right corner under Related Links, to either Run License Report or View License Usage. The first report lists any license violations. The second report lists all license counts.

CHAPTER 6

User and Administrator Access

This chapter contains the following sections:

Cisco Unity Connection Does Not Respond to Touchtones

When Cisco Unity Connection is integrated by SCCP to Cisco Unified CallManager, Cisco Unity Connection may not respond to touchtones.

In certain situations, DTMF digits are not recognized when processed through VoIP dial-peer gateways. To avoid this problem, certain gateways must be configured to enable DTMF relay. The DTMF relay feature is available in Cisco IOS software version 12.0(5) and later.

Cisco IOS software-based gateways that use H.245 out-of-band signaling must be configured to enable DTMF relay.

The Catalyst 6000 T1/PRI and FXS gateways enable DTMF relay by default and do not need additional configuration to enable this feature.

To Enable DTMF Relay

Step 1 On a VoIP dial-peer servicing Connection, use the following command:

```
dtmf-relay h245-alphanumeric
```

Step 2 Create a destination pattern that matches the Cisco Unified CallManager voice mail port numbers. For example, if the system has voice mail ports 1001 through 1016, enter the dial-peer destination pattern 10xx.

Step 3 Repeat Step 1 and Step 2 for all remaining VoIP dial-peers servicing Connection.

Cisco Personal Communications Assistant Pages Are Incomplete or Blank

An incomplete Cisco Personal Communications Assistant page may be empty or partially empty because of an error in the processing of the dynamic elements contained in the page. Such errors can be caused by one or more of the following:

- An error in the data collection processing for the requested page (server side)
- An error in the data rendering processing of the requested page (server side)
- An error in the processing of the dynamic scripting in the page (client side)

To correct the problem, you will need to reinstall the Cisco Unity Connection system. See the *Cisco Unity Connection Installation Guide* for procedures and information. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Before you attempt to reinstall Cisco Unity Connection, gather the data that you may need to provide to Cisco TAC in the event that reinstalling Connection does not resolve the problem. Do the following:

- To assist in diagnosing data processing errors on the server side, collect the log files for Cisco PCA that cover the time when the issue occurred. The file names for these files start with "ciscopca_" and can be found in the "%CU_HOME%\logs" folder.
- To assist in diagnosing errors in the processing of the dynamic scripting in the page on the client side, try to collect a screen capture of the browser that shows the issue, and a text file containing the source code for the incomplete or blank page (however, note that if the Cisco PCA uses an SSL connection, you may not be able to save the source code).

If you are confident the issue resides on the server side, collecting the client information will still help Cisco TAC to determine the exact issue and provide a solution or workaround faster.

If the problem is that the Media Master control bar does not show up correctly or at all, see the "Media Master" chapter.

Users Cannot Access Cisco Personal Communications Assistant Pages

Users use the Cisco PCA website to access the Cisco Unity Assistant, the Cisco Unity Inbox, and the Cisco Unity Personal Call Transfer Rules pages.

When a user cannot access the Cisco Personal Communications Assistant pages, consider the following possible causes. Additional troubleshooting information and procedures are available in the "Cisco Personal Communications Assistant" chapter.

URL Is Case-Sensitive

Users can access the Cisco PCA at the following URL: http://<Cisco Unity Connection server>/ciscopca. Note, however, that the URL is case-sensitive.

Incorrect Browser or Client Configuration

When a user cannot access any of the Cisco PCA pages, it may be that the user browser or client workstation is not configured properly. Make sure that the browser and client workstation are configured as specified in the *Cisco Unity Connection User Setup Guide*. (The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.)

Unsupported Software Is Installed on Client Workstation

Confirm that the user does not have an unsupported combination of software or an unsupported third-party application installed on the workstation. See the *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations*, available at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.

Cisco Unity Connection Uses SSL but the Certificate Has Not Been Distributed to the Trusted Root Store

If you installed an SSL certificate on the Cisco Unity Connection server to secure Cisco PCA access to Connection, you probably will also want to add the certificate to the Trusted Root Store on user workstations. If you do not install the certificate on user workstations, users can use Cisco PCA, but the web browser will display a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Connection may also display this warning message if the URL used to connect to the Connection server is different from the hostname of the server at the time the Connection software was installed.

If you installed an SSL certificate to secure IMAP e-mail client access to Connection, you may need to add the certificate to the Trusted Root Store on user workstations. Some of the IMAP e-mail clients supported for use with Connection display SSL security messages, while others do not.

For situations where the client computer is running Windows Server 2003 and a user is using Internet Explorer 6.0 to access the Cisco Personal Communications Assistant, provide the user with the following "To Add the Cisco Unity Connection Server to the List of Trusted Sites for Internet Explorer 2003" procedure to add the Cisco Unity Connection server to the list of Trusted Sites. These additional configuration steps must be performed for these user workstations in order for the Cisco PCA to work correctly.

To Add the Cisco Unity Connection Server to the List of Trusted Sites for Internet Explorer 2003

Step 1 Open the Cisco Personal Communications Assistant Login page. It is not necessary to log in to the Cisco PCA.

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

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

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

Step 5 Restart Internet Explorer.

Users Cannot Access the Cisco Unity Assistant, Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules from the Cisco PCA

When users can access the Cisco PCA, but cannot access the Cisco Unity Assistant, the Cisco Unity Inbox, or the Cisco Unity Personal Call Transfer Rules, consider the following possible causes:

- In order to access the Cisco Unity Assistant, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Assistant" setting enabled.

- The Cisco Unity Inbox is a licensed feature, and can be accessed only if it is purchased. In addition, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Inbox" setting enabled.
- In order to access the Cisco Unity Personal Call Transfer Rules, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service must have the "Allow Users to Use the Cisco Unity Personal Call Transfer Rules" setting enabled.

Users Cannot Save Changes on Pages in the Cisco Unity Assistant, Cisco Unity Inbox, or the Cisco Unity Personal Call Transfer Rules

When user browser settings are set to cache temporary Internet pages automatically, users can create a bookmark or Favorite to access a Cisco Unity Assistant, Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules web page, but the page will be read-only. Explain to users that they should bookmark the Cisco PCA home page, rather than individual pages. (Users should not change their browser settings as a workaround; when the browser is not set to automatically check for newer versions of temporary Internet files, the Media Master control is not displayed correctly.)

Voice Mail Users Cannot Be Located in a Directory Handler

Callers may report that they are unable to locate one or more users in a directory handler.

For users to be located in a directory handler, they must have a recorded name, and must be configured to be listed in the directory.

Verify the List in Directory setting on the Edit User Basics page for the user in Cisco Unity Connection Administration.

Internal and External Calls

This chapters contains the following sections:

- Cisco Unity Connection Is Not Answering Any Internal and/or External Calls, page 7-1
- Cisco Unity Connection Is Not Answering Some Internal or External Calls, page 7-2

Cisco Unity Connection Is Not Answering Any Internal and/or External Calls

When the phone system settings in Cisco Unity Connection Administration do not match the type of phone system that Connection is connected to, Connection may not answer calls.

To Confirm the Phone System Settings in Cisco Unity Connection Administration

Step 1 Log on to Cisco Unity Connection Administration.

Step 2 Expand **Telephony Integrations**.

Step 3 Confirm that the settings for the phone system, port groups, and ports match those indicated in the integration guide for your phone system.

Step 4 Correct any incorrect values in Connection Administration.

Step 5 If you change any values, click **Save**.

Step 6 If prompted to restart Connection, in the Windows task bar, right-click the **Connection** icon and click **Restart > Voice Processing Server Role**.

Step 7 In Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **Go** to confirm the phone system integration settings.

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

Step 8 In the Task Execution Results window, click **Close**.

Step 9 Log off Connection Administration.

Cisco Unity Connection Is Not Answering Some Internal or External Calls

There are two possible reasons that Cisco Unity Connection may not answer some internal and/or external calls. Use the "Task List for Troubleshooting Sporadic Answers on Incoming Calls" to troubleshoot the possible causes.

Task List for Troubleshooting Sporadic Answers on Incoming Calls

1. Confirm that the routing rules are working correctly. See the "Confirming Routing Rules" section on page 7-2.
2. Confirm that calls are sent to the correct voice messaging ports and that the ports are enabled. See the "Confirming Voice Messaging Port Settings" section on page 7-3.

Confirming Routing Rules

By default, Cisco Unity Connection does not reject any calls. If routing rules have been changed, Connection may have been unintentionally programmed to reject some internal or external calls.

To Confirm That Cisco Unity Connection Routing Rules Are Working Correctly

Step 1 On the Cisco Unity Connection desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane of the Tools Depot window, under Diagnostic Tools, double-click **Unity Diagnostic Tool**.

Step 3 In the Cisco Unity Diagnostic Tasks pane, click **Configure Micro Traces**.

Step 4 On the Configure Micro Traces Wizard Welcome screen, click **Next**.

Step 5 Expand **Arbiter**.

Step 6 Under Arbiter, check the three call routing check boxes (components **14**, **15**, and **16**).

Step 7 Expand **Routing Rules**.

Step 8 Under Routing Rules, check the **Rules Creation/Deletion/Evaluation** check box (component **11**).

Step 9 Click **Next**.

Step 10 Click **Finish**.

Step 11 Reproduce the problem.

Step 12 To view the log files, in the left pane of the Cisco Unity Diagnostics screen, expand **Cisco Unity Diagnostic Tool >Processes > CuCsMgr**, and then click the current log file.

The selected log file is formatted and displayed in the right pane.

Step 13 To save a copy of the log file, right-click the file in the left pane, and click **All Tasks > Gather Log Files**, then follow the prompts in the Gather Logs Wizard.

Step 14 To turn off the traces set in Step 6 and Step 8, right-click **Cisco Unity Diagnostic Tool**, and click **All Tasks > Reset to Default Traces**.

Step 15 To view the actual conditions of routing rules, go to the Call Management > Call Routing pages in Cisco Unity Connection Administration. Compare the conditions of the routing rules with the information gathered from the diagnostic file to see why a rule is applied to a call.

Step 16 Use the Call Management > Call Routing pages to modify routing rules, as applicable.

If you are unable to determine if routing rules are the source of the problem, or if you need assistance interpreting the information in the diagnostic logs, contact Cisco TAC.

Confirming Voice Messaging Port Settings

If the phone system is programmed to send calls to a voice messaging port on Cisco Unity Connection that is not configured to answer calls, Connection will not answer the call.

To Confirm That Calls Are Being Sent to the Correct Voice Messaging Ports on Connection

Step 1 Log on to Cisco Unity Connection Administration.

Step 2 Expand **Telephony Integrations**, then click **Port**.

Step 3 On the Search Ports page, note which ports are designated to answer calls.

Step 4 On the phone system, in the phone system programming, confirm that calls are being sent only to those voice messaging ports designated to answer calls. Change the phone system programming if necessary.

Step 5 If you made a change to the phone system programming in Step 4, in the Windows task bar, right-click the **Connection** icon and click **Restart > Voice Processing Server Role**. Restarting the Voice Processing Server role will clear any hung ports.

Step 6 Log off Connection Administration.

If a voice messaging port is disabled or set incorrectly, it will not answer calls.

To Confirm That Voice Messaging Ports Are Enabled

Step 1 Log on to Cisco Unity Connection Administration.

Step 2 Expand **Telephony Integrations**, then click **Port**.

Step 3 If a voice messaging port is not enabled and should be in use, on the Port Basics page for the port, check the **Enabled** check box to enable the port.

CHAPTER 8

Call Transfers

This chapter contains the following sections:

- Calls Are Not Transferred to the Correct Greeting, page 8-1
- Administering Alternate Extensions, page 8-3

Note For call transfer problems that occur on newly installed systems, see the applicable Cisco Unity Connection integration guide.

If you encounter a call transfer problem that is not described in this chapter, contact the Cisco Technical Assistance Center (TAC).

Calls Are Not Transferred to the Correct Greeting

The following sections describe possible reasons that calls may not be transferred to the correct greeting. Use the "Task List for Troubleshooting Call Transfers to the Wrong Greeting" to troubleshoot the possible causes.

Task List for Troubleshooting Call Transfers to the Wrong Greeting

1. Confirm that the forward timer in the phone system is synchronized with the Rings to Wait For setting in Cisco Unity Connection. See the "Confirming That the Forward Timer in the Phone System Is in Synch with the Rings to Wait For Setting in Cisco Unity Connection" section on page 8-1.
2. Confirm that the phone system programming enables callers to hear the personal greeting of the user. See the "Confirming That the Phone System Integration Enables Playing the User Personal Greeting for Callers" section on page 8-3.

Confirming That the Forward Timer in the Phone System Is in Synch with the Rings to Wait For Setting in Cisco Unity Connection

For supervised transfers, the number of rings that Cisco Unity Connection waits before routing a call to a user personal greeting (or to another extension) can be reconfigured. If the phone system is programmed to forward calls, confirm that the phone system waits longer to forward a call than Connection waits before taking a message.

If the phone system is forwarding the call to another extension before Connection can take a message, the following may occur:

- The caller does not hear the beginning of the user personal greeting. (For example, the user greeting is "Hi, this is Maria Ramirez. Please leave a message after the tone." But the caller hears only "...message after the tone.")
- The call is forwarded to another phone (for example, the operator) rather than to the personal greeting of the user.
- The call is forwarded to the opening greeting.
- The caller hears only ringing.

To Synchronize the Forward Timer and the Rings to Wait For Setting

Step 1 In the phone system programming, find and note the setting of the forward timer.

Step 2 In Cisco Unity Connection Administration, expand **Users**, then click **Users**.

Step 3 On the Search Users page, click the alias of the user whose calls are not being routed to the correct greeting.

Step 4 On the Edit User Basics page, on the Edit menu, click **Transfer Options**.

Step 5 On the Transfer Options page, click the name of the active transfer option.

Step 6 On the Edit Transfer Option page, under Transfer Action, confirm that the **Extension** option is selected for the Transfer Calls To field and that the extension number is correct.

Step 7 In the Transfer Type drop-down box, confirm that **Supervise Transfer** is selected.

Step 8 In the Rings to Wait For field, the setting should be two rings fewer than the setting of the forward timer of the phone system, which you noted in Step 1. This setting is typically not greater than four. It specifies the number of rings that Cisco Unity Connection waits before routing the call to the personal greeting of the user.

If the settings do not meet the parameters, either reprogram the phone system so that it waits longer before forwarding unanswered calls, or change the Rings to Wait For field setting so that Cisco Unity Connection routes the call before the phone system forwards it.

Step 9 Click **Save**.

Step 10 To change the default Rings to Wait For value for future users, expand **Templates** and click **User Templates**.

Note If you change settings in a user template, the settings are not changed for existing users. Changing the template settings affects only the users who are added after the template changes are made.

Step 11 On the Search User Templates page, click the alias of the user template that you want to change.

Step 12 On the Edit User Template Basics page, on the Edit menu, click **Transfer Options**.

Step 13 On the Transfer Options page, click the name of the active transfer option.

Step 14 On the Edit Transfer Option page, under Transfer Action, confirm that the **Extension** option is selected for the Transfer Calls To field.

Step 15 In the Transfer Type drop-down box, confirm that **Supervise Transfer** is selected.

Step 16 In the Rings to Wait For field, enter the same setting that you entered in Step 7.

Step 17 Click **Save**.

Confirming That the Phone System Integration Enables Playing the User Personal Greeting for Callers

When callers hear the opening greeting instead of the user personal greeting, confirm that the phone system integration is correctly set up. If the settings are not correct, call forward to personal greeting and easy message access will not be enabled. Do the following procedure.

To Verify the Phone System Integration Settings

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

Step 2 Confirm that the settings for the phone system, port group, and ports match those indicated in the applicable Cisco Unity Connection integration guide.

Step 3 Correct any incorrect settings for the phone system integration.

Step 4 If you have confirmed that the phone system integration settings are correct, and callers still hear the opening greeting after dialing the user extension, contact Cisco TAC.

Administering Alternate Extensions

Giving users alternate extensions can make calling Cisco Unity Connection from an alternate device—such as a mobile phone, a home phone, or a phone at another work site—more convenient. When you specify the phone number for an alternate extension, Connection handles all calls from that number in the same way that it handles calls from the primary extension of the user (assuming that the alternate phone number is passed along to Connection from the phone system).

This means that Connection associates the alternate phone number with the user account. When such phones are set to forward to Connection, callers will hear the user greeting and leave messages for the user, just as they would when dialing the primary extension of the user.

To administer alternate extensions for users, in Cisco Unity Connection Administration, click Users and search for the user. On the Edit User Basics page, on the Edit menu, click Alternate Extensions.

CHAPTER 9

Messages

This chapter contains the following sections:

- IMAP E-Mail Access to Cisco Unity Connection Voice Mail, page 9-1
- Message Quota Enforcement: Responding to Full Mailbox Warnings, page 9-2
- Undeliverable Messages, page 9-2
- Messages Appear to Be Delayed, page 9-3
- Some Messages Seem to Disappear, page 9-3
- Cisco Unity Connection Stops Recording Before a Caller Has Finished Leaving a Message, page 9-5
- Secure Messages, page 9-6

IMAP E-Mail Access to Cisco Unity Connection Voice Mail

See the following sections:

- Changing Passwords, page 9-1
- Troubleshooting Logon Problems with IMAP E-Mail Clients, page 9-1

Changing Passwords

If users change a Cisco Unity Connection password from the Cisco Unity Assistant, they also must update this password from their IMAP e-mail client application so that the client can continue to access Connection and retrieve voice messages.

Troubleshooting Logon Problems with IMAP E-Mail Clients

If users have trouble receiving voice messages to their IMAP client, consider the following information:

- If the IMAP client application prompts a user for the Cisco PCA password, but does not accept it, the Cisco PCA password may have expired or changed, or is locked. Users can change their password from the Cisco Unity Assistant first and then update it from their IMAP client application.

- If Microsoft Outlook users are not prompted for their Cisco PCA password, verify that the Remember Password check box on the Internet E-mail Settings (IMAP) page is not checked. If this option is checked, and the password of the user has expired, changed, or is locked, Microsoft Outlook will not prompt the user to enter the Cisco PCA password. The result is that the user will not receive voice messages from Connection.

Message Quota Enforcement: Responding to Full Mailbox Warnings

When users hear a prompt about a full mailbox, it means that one or more of the three quotas that limit the size of voice mailboxes has been reached:

- If a mailbox has reached the size of the warning quota, the user will hear a warning that the mailbox is almost full.
- If a mailbox has reached the size of the send quota, the user will be unable to send messages and will hear that messages cannot be sent. If the user belongs to the correct class of service and has deleted messages in the mailbox, Cisco Unity Connection will offer the option to remove all deleted messages.
- If a mailbox has reached the size of the send and receive quotas, the user will experience the same conditions as the send quota and in addition will not be able to receive new messages. Unidentified caller messages will not be allowed, and messages from other users will generate nondelivery receipts to the senders. To decrease the size of the mailbox, the user can remove all deleted messages and/or remove saved or new messages individually until the mailbox size is below the quotas.

Undeliverable Messages

Occasionally, messages cannot be delivered to the recipient that the caller intended to reach. The system behavior in this case depends on the type of sender and the reason that the message could not be delivered.

In general, if Connection cannot deliver the message because of issues that are not likely to be resolved (for example, the caller was disconnected before addressing the message, or the recipient mailbox has been deleted), the message is sent to the Undeliverable Messages distribution list, and Connection sends a nondelivery receipt (NDR) to the sender.

Note that the sender will not receive a nondelivery receipt in the following cases:

- When the sender of the original message is an unidentified caller
- When the sender is a user, but the user is configured to not accept NDRs
- While the Microsoft SQL Server database is down (in this case, the NDR will be delivered when the database becomes available)

However, if the original message is malformed or contains non-voice messaging content, instead of sending the message to the Undeliverable Messages list, Connection will place the message in the MTA bad mail folder (UmssMtaBadMail). This folder is automatically checked nightly by the Monitor Bad Mail Folders task, and if messages are found, an error is written to the application event log indicating troubleshooting steps.

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

Messages Appear to Be Delayed

Use the "Task List for Troubleshooting Delay in Appearance of Messages" to troubleshoot the possible causes for the apparent delay of messages.

Task List for Troubleshooting Delay in Appearance of Messages

1. To confirm the arrival times of messages, generate a user message activity report for the user. For more information, see the "Generating System Configuration and Call Management Reports" chapter in the *Cisco Unity Connection System Administration Guide*, *Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
2. See the applicable information in the "Orientation Task List" section of the "User Orientation" chapter of the *Cisco Unity Connection User Setup Guide, Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Some Messages Seem to Disappear

Use the "Task List for Troubleshooting the Disappearance of Some Messages" to troubleshoot the possible causes for messages not being delivered to the intended recipients.

Task List for Troubleshooting the Disappearance of Some Messages

1. Verify that users who are assigned to the Undeliverable Messages distribution list have been forwarding messages to the intended recipients. See the "Undeliverable Messages Have Not Been Forwarded to Recipients" section on page 9-4.
2. Verify that the user mailbox is not full. See the "A User Has a Full Mailbox" section on page 9-3.
3. Confirm that you or another administrator did not inadvertently delete a user who was assigned to review the messages for Connection entities. See the "Users Assigned to Cisco Unity Connection Entities Were Deleted and No Replacements Were Assigned" section on page 9-4.
4. *If McAfee VirusScan is installed on the Connection server:* Confirm that the default setting to block traffic on SMTP port 25 has been changed. Blocking traffic on SMTP port 25 prevents Connection from delivering voice messages to user inboxes. See the "McAfee VirusScan Is Blocking Traffic on SMTP Port 25" section on page 9-5.
5. Review message aging settings. See the "Message Aging Policy" chapter in the *Cisco Unity Connection System Administration Guide*, at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

A User Has a Full Mailbox

If a user mailbox is no longer allowed to receive messages, Cisco Unity Connection handles the message in one of the two following ways:

- By default, if an outside caller attempts to send a message to a user whose send/receive quota has been exceeded, Connection will indicate to the caller that the recipient mailbox is full, and will not allow the caller to record a message for the recipient.

  If the recipient mailbox has not yet exceeded the send/receive quota at the time an unidentified caller records a message, but the quota is exceeded in the act of delivering the message, Connection will deliver the message regardless of the quota.

- If a user whose voice mailbox has exceeded the send quota logs in to Connection and attempts to send a message to another user, Connection will indicate that the send quota has been exceeded, and will not allow the sender to record the message. If the user calls another user and is forwarded to a voice mailbox, the user will be able to leave a message, but the message will be sent as an outside caller message.

  If a user attempts to send a message to another user whose mailbox has exceeded the send/receive quota, or if the quota is exceeded in the act of delivering the message, Connection will send a nondelivery receipt to the message sender.

  Connection delivers read receipts and nondelivery receipts to users regardless of whether their quotas have been exceeded.

Encourage the user to dispose of messages promptly so that the Connection mailbox does not fill up, and explain to users on the Undeliverable Messages distribution list the importance of regularly checking for and forwarding undeliverable messages.

Caution If the mailbox(es) of the user(s) who are assigned to check the Undeliverable Messages list exceed the send/receive quota, the messages sent to the Undeliverable Messages distribution list are lost. To avoid this problem, specify a generous value for the send/receive quota for at least one user who is a member of the Undeliverable Messages list, and encourage the user to dispose of messages promptly.

Undeliverable Messages Have Not Been Forwarded to Recipients

Messages returned to the Unity Messaging System mailbox are forwarded automatically to users whose names appear on the Undeliverable Messages system distribution list. The messages then must be forwarded to the intended recipients. Explain to users on the Undeliverable Messages distribution list the importance of regularly checking for and forwarding undeliverable messages.

Caution If the mailbox(es) of the user(s) who are assigned to check the Undeliverable Messages list exceed the send/receive quota, the messages sent to the Undeliverable Messages distribution list are lost. To avoid this problem, specify a generous value for the send/receive quota for at least one user who is a member of the Undeliverable Messages list, and encourage the user to dispose of messages promptly.

Users Assigned to Cisco Unity Connection Entities Were Deleted and No Replacements Were Assigned

When you delete a user who was assigned to review the messages sent to any of the following Cisco Unity Connection entities, make sure that you assign another user or a distribution list to replace the deleted user; otherwise, messages may be lost.

- Undeliverable Messages distribution list (by default, the UndeliverableMessagesMailbox user account is the only member of this distribution list)

- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

McAfee VirusScan Is Blocking Traffic on SMTP Port 25

By default, McAfee VirusScan Enterprise blocks traffic on SMTP port 25, which prevents Cisco Unity Connection from delivering voice messages to user inboxes. When this occurs, you may see the following error in the Windows application event log:

Event Type: Error
Event Source: CiscoUnity_CsMalUmss
Event Category: Error
Event ID: 1004
Date: <date>
Time: <time>
User: N/A
Computer: <server name>
Description: The SMTP service on localhost:25 is not responding and is unable to deliver messages. The SMTP service may be down. Messages will accumulate in [drive letter]:\UC_Mailroot\UmssCsMalQueue until this is resolved. Verify that the SMTP service is running.

To change the setting in VirusScan, do the following procedure. Note that the procedure is current as of the time this document was written. The VirusScan user interface may change.

To Stop McAfee VirusScan from Blocking Traffic on SMTP Port 25

Step 1 Start McAfee VirusScan Console.

Step 2 Right-click **Access Protection**, and click **Properties**.

Step 3 In the Access Protection Properties dialog box, on the Port Blocking tab, in the Ports to Block list, confirm that the **Prevent Mass Mailing Worms From Sending Mail** check box is unchecked.

Step 4 Click **OK** to close the Properties dialog box.

Step 5 Close the VirusScan Console.

Cisco Unity Connection Stops Recording Before a Caller Has Finished Leaving a Message

If a caller reports being cut off while leaving a message and if the caller did not hear a prompt prior to the disconnect, Cisco Unity Connection, the phone system, or the central office may have disconnected the call.

To Determine Why the Call Was Disconnected

Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.

Step 2 In the left pane of Event Viewer, click **System Log**.

Step 3 In the system event log, look for an error that occurred at the time of the reported disconnected call.

If an error appears, double-click the error and skip to Step 6.

If no error appears for the date and time of the disconnected call, continue with Step 4.

Step 4 In the left pane, click **Application Log**.

Step 5 In the application event log, look for an error that occurred at the time of the reported disconnected call. Double-click the error.

Step 6 In the Event Detail dialog box, review the contents of the Description box.

If you need assistance interpreting or resolving the error, or if no error appears in the application event log that matches the date and time of the reported disconnected call, contact Cisco TAC.

Secure Messages

A user who is enabled to send encrypted secure messages will hear "To mark this private and secure, press 3" in the Cisco Unity Connection conversation while sending a message. The message will be encrypted, and marked private to prevent it from being forwarded. A user who is not enabled to send encrypted secure messages will instead hear "To mark this private, press 3," which will prevent the message from being forwarded. A user also can mark a message both private and secure in the Cisco Personal Communications Assistant.

A user may not need to explicitly mark a message for encryption. There are several system-level settings that control whether a message is encrypted. A system-level setting can be enabled so that all user-to-user messages are encrypted or that all outside-caller messages are encrypted.

See the following troubleshooting sections for more information on these issues:

- An encryption or decryption error results in the generation of an Event log error message. See the "Decryption Event Log Error Messages" section on page 9-6 or the "Encryption Event Log Error Messages" section on page 9-7, as applicable.
- A user hears the failsafe conversation or the decoy WAV file. See the "Users Hear the Failsafe Conversation or the Decoy WAV File" section on page 9-7.

Note For more information on private and secure messaging, see the "Setting Up Private and Secure Messaging" chapter of the *Cisco Unity Connection System Administration Guide*, *Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Decryption Event Log Error Messages

Decryption errors can be caused by the following:

- The voice message was not encrypted with the public key.
- The private key is missing, invalid, or unable to be used.
- There is another problem with the key.

In all of these cases, start by creating a new certificate. Then ask the sending user to re-record the voice message, if applicable.

Error Message `A private secure message from %ss to %sr could not be decrypted, possibly because the message was not encrypted with the public key for this server or there is a problem with the private key on this server.`

Recommended Action Install a new certificate on the Connection server, and restart Connection services. If this does not resolve the problem, contact Cisco TAC.

Encryption Event Log Error Messages

Encryption errors are caused by a problem with the public key. For example, the public key may be missing, invalid, or unusable. Start by creating a new certificate. Then ask the sending user to re-record the voice message, if applicable.

Error Message `A private secure message from %ss could not be encrypted because a valid public key could not be found on this server.`

Recommended Action Create a new certificate on this server, then ask the sending user to re-record the voice message. If creating a new certificate on this server does not resolve the problem, contact Cisco TAC.

Error Message `A private secure message from %ss could not be encrypted, possibly because there is a problem with the public key on this server.`

Recommended Action Create a new certificate on this server, then ask the sending user to re-record the voice message. If creating a new certificate on the sending server does not resolve the problem, contact Cisco TAC.

Users Hear the Failsafe Conversation or the Decoy WAV File

If a user hears the failsafe conversation ("Sorry, this system is temporarily unable to take your call") when attempting to send a secure voice message, encryption of the message may have failed. Review the Windows application event log to determine the cause. When an encryption attempt fails, the voice message is deleted and cannot be recovered. The user must re-record the message.

If a user hears the following decoy WAV file when attempting to listen to a secure voice message by phone, decryption of the message may have failed:

> "This voice message is private and secure and can only be played if you log on to the voice mail system and check your messages by phone. If you received this message in error, notify the sender and delete it immediately."

Review the application event log to determine the cause. When a decryption attempt fails, in most cases the voice message will not be playable, even after the problem has been resolved. For example, when problem resolution requires creation of a new certificate on the Connection server, then the sending user must re-record the message.

Text to Speech

This chapter contains the following sections:

Diagnostic Traces for Text to Speech

To help diagnose problems with TTS and the IMAP connection to Exchange, the following micro traces can be turned on in the Cisco Unity Diagnostic Tool:

- Common Messaging Layer (CML) > CML Session Trace
- Common Messaging Layer (CML) > CML IMAP Messaging Trace

The diagnostics will be found in the diag_cuscmgr*.* file.

Options Allowed While Listening to E-Mail

While listening to e-mail with Text to Speech (TTS), users have the same options allowed with voice messages, except for the following, which are not allowed for e-mail:

- Reply (includes live reply and reply to all)
- Forward
- Individually hard delete

  Users can hard delete all soft-deleted e-mail at once through the same conversation they would use to permanently remove all soft-deleted voice messages.

Users Hear Gibberish at the End or Beginning of an E-Mail

When users hear gibberish at the end or beginning of an e-mail, the gibberish is part of the e-mail formatting that TTS plays back. Although the TTS engine is able to clean up some of the gibberish that can be found in various e-mail formats, there are formats that will cause some gibberish to be played.

E-Mail Deleted by Phone Is Still in the Inbox Folder

When accessing an e-mail account with a MAPI client (such as Microsoft Outlook 2000), e-mail that was deleted by phone may still appear in the Inbox and not in the Deleted Items folder.

Cisco Unity Connection uses the IMAP protocol to interact with Microsoft Exchange. Microsoft Exchange handles messages that are soft-deleted via IMAP differently than those that are soft-deleted by using the MAPI protocol. When a message is soft-deleted through IMAP, it is marked as deleted and left in the Inbox folder. When a message is soft-deleted through MAPI, it is moved to the Deleted Items folder.

Short Delays or No Access While Listening to E-Mail

While listening to e-mail with TTS, a user may experience up to a four-second delay, or a user may be told that e-mail could not be read. This behavior may be intermittent.

Cisco Unity Connection allows itself four seconds to contact the Microsoft Exchange server and respond to any given IMAP request. If there are network or Exchange issues, Connection will abort the task to avoid any long delays in the conversation. If network problems happen at logon, e-mail will not be available for the duration of the call. If network problems happen during message access, further e-mail may not be read for the duration of the call, or the caller may hear the failsafe prompt.

Microsoft Exchange can respond slowly for a number of reasons, but the most common reason is that the user has a large number of messages in their Inbox folder (for example, more than 1000 messages). One solution may be to have the user delete messages or reorganize their e-mail folders to reduce the number of messages in the Inbox.

Another solution is to increase the amount of time Connection waits to access TTS before timing out. In Cisco Unity Connection Administration, expand System Settings > Advanced > Conversations and change the setting for Maximum Delay for TTS Access Before Timeout from the default setting of 4 seconds to 6 or 10 seconds. Increasing the timeout value will give Exchange more time to respond to IMAP requests and successfully retrieve messages, but callers may experience long pauses while waiting for the system to respond.

The diagnostics in the diag_cuscmgr*.* file should give an indication of what the problem was.

User Is Configured for TTS, But E-Mail Is Not Offered to the User

This issue is normally due to Cisco Unity Connection not being able to contact or establish an authenticated connection with Microsoft Exchange. With this issue, all TTS-enabled users on the system are affected, rather than just a few.

Do the following to troubleshoot this issue:

1. In Cisco Unity Connection Administration, confirm that all of the information provided for the External Service defined for the Microsoft Exchange server is correct. In Cisco Unity Connection Administration, expand System Settings > External Services and select the defined external service. In particular, confirm that the Server Name, Service Login, and Service Password values are correct. For the Service Login value, confirm that this is formatted as "<domain>\<username>."
2. Confirm that the affected users have the correct mailbox name defined for their IMAP external service account. To do this, in Cisco Unity Connection Administration, go to the External Service Accounts page for each affected user and select the IMAP external service account.
3. Confirm that the server address defined for the Exchange server in the Connection Administration can be used at the Cisco Unity Connection server command line to ping the Microsoft Exchange server.
4. If you have confirmed the information in the above steps, and users are still unable to access e-mail, try changing the "Security Transport" setting for the external service from SSL to None. In Cisco Unity Connection Administration, expand System Settings > External Services and select the defined external service. After changing the Security Transport setting, try accessing e-mail from the phone conversation. If TTS access is working, then this indicates that the common name (CN) on the Exchange Server SSL certificate may be different than the value provided as the "DNS Address of Server" defined for the external service in Cisco Unity Connection Administration. These names must match exactly in order for Cisco Unity Connection to trust the certificate it receives from Microsoft Exchange.

Note When you change the Security Transport setting for the external service from SSL to None, check to see that Exchange is set to allow non-SSL connections for IMAP. If you only allow SSL connections for IMAP, you may need to temporarily disable the "Requires SSL/TLS Encryption" setting on the Authentication page for the Default IMAP4 Virtual server to assist in isolating the problem.

Message Notifications

This chapter includes the following sections:

Message Notification Is Slow for Multiple Users

There are several possible reasons that message notification may appear to be slow for multiple users. Use the "Task List for Troubleshooting Slow Message Notifications for Multiple Users" to troubleshoot the possible causes.

Task List for Troubleshooting Slow Message Notifications for Multiple Users

1. Confirm that ports are not too busy to handle message notification. See the "Ports Are Too Busy to Make Notification Calls Promptly" section on page 11-1.
2. Confirm that there are enough ports assigned to message notification. See the "Not Enough Ports Are Set for Message Notification Only" section on page 11-2.
3. Confirm that the phone system sends calls to ports that are set to answer calls. See the "Confirming That the Phone System Sends Calls to the Ports Set to Answer Calls" section on page 11-2.

Ports Are Too Busy to Make Notification Calls Promptly

When the ports that make notification calls are also set to perform other operations, they may be too busy to make notification calls promptly. You can improve notification performance by dedicating a smaller number of ports to making notification calls exclusively.

Systems that handle a large volume of calls may require additional ports to improve notification performance.

To Review Port Configuration for Message Notification

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integration**, then click **Port**.

Step 2 Review the existing port configuration and determine whether one or more ports can be set to dial out for message notification only.

Not Enough Ports Are Set for Message Notification Only

When a small number of ports are set to make notification calls and Cisco Unity Connection takes a lot of messages, the notification ports may not always be able to dial out promptly.

If the percentage of ports used for dialing out for message notification exceeds 70 percent usage during peak periods, review the existing port configuration and determine whether more ports can be set to dial out for message notification only.

If the percentage of ports used for dialing out for message notification does not exceed 70 percent usage during peak periods, the number of notification ports is adequate. Contact Cisco TAC to resolve the problem.

To Determine Whether the Number of Message Notification Ports Is Adequate

Step 1 On the Windows desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Reporting Tools, double-click **Port Usage Analyzer**.

Step 3 In the Port Usage Analyzer window, click the **Port Availability** tab.

Step 4 In the Data Logs Folder field, enter the path to the data logs.

Step 5 In the Select Day list, click the day for which you want port usage analyzed.

Step 6 Click **Load Data**. A summary of the port usage information appears in a dialog box.

Step 7 (Optional) To generate a report, on the Port Availability tab, click **Run Report**.

Step 8 If the percentage of ports used exceeds 70 percent usage during peak periods, in Cisco Unity Connection Administration, expand **Telephony Integration**, then click **Port**. Then skip to Step 9.

If the percentage of ports used does not exceed 70 percent usage during peak periods, the number of message waiting indication ports is adequate.

Step 9 Review the existing port configuration and determine whether more ports can be set to dial out for message notification only.

Confirming That the Phone System Sends Calls to the Ports Set to Answer Calls

If the phone system is programmed to send calls to a port on Cisco Unity Connection that is not configured to answer calls, Connection will not answer the call.

To Confirm That Calls Are Being Sent to the Correct Cisco Unity Connection Ports

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integration**, then click **Port**.

Step 2 Note which ports are set to answer calls.

Step 3 In the phone system programming, confirm that calls are only being sent to ports set to answer calls. Change the phone system programming if necessary.

Step 4 If you make a change to the phone system programming, restart the Connection server to clear any hung ports.

Message Notification Is Slow for a User

There are several possible reasons that message notification may appear to be slow for a user. Use the "Task List for Troubleshooting Slow Message Notification for a Single User" to troubleshoot the possible causes.

Task List for Troubleshooting Slow Message Notification for a Single User

1. The user settings may not be adequate for the needs of the user. See the "Message Notification Setup Is Inadequate" section on page 11-3.
2. The user settings may need adjustment to more correctly map to the work schedule of the user. See the "Notification Attempts Are Missed" section on page 11-4.
3. The user may not clearly understand how repeat notifications are handled by Connection. See the "Repeat Notification Option Is Misunderstood" section on page 11-4.

Message Notification Setup Is Inadequate

When a user complains that notification calls are not being received when expected, the problem may be with the notification settings.

To Determine Whether Notification Setup Is Adequate

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 Confirm with the user that the notification device is applicable to the needs of the user. If the user has selected a very busy phone for Connection to call, ask if there is an alternate phone or pager to use for message notification.

Step 6 Confirm with the user that the notification schedule is consistent with the days and times that the user is available to receive notification calls.

Notification Attempts Are Missed

A user who is frequently away from or busy using a notification device may repeatedly miss notification attempts. To the user, it appears that Cisco Unity Connection has delayed message notification.

To Resolve Missed Notification Attempts

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 In the Notification Event list, click **Every Voice Mail**.

Step 6 Check the **Repeat Notification If There Are Still Messages** check box.

Step 7 If the user has another notification device available, for On Notification Failure, click **Send To**, and choose the device.

Step 8 In the Busy Retry Limit and RNA Retry Limit boxes, increase the numbers so that Connection makes more notification calls when the device does not answer or is busy.

Step 9 In the Busy Retry Interval and RNA Retry Interval boxes, decrease the numbers so that Connection makes notification calls more often when the device does not answer or is busy.

Step 10 Click **Save**.

Step 11 If you chose another device in Step 7:

a. On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

b. In the Device list, click the correct notification device.

a. Enter settings and a schedule for the additional device.

Step 12 Suggest that the user set up an answering machine for the notification phone, so that notification calls are received even when the user is unavailable.

When Connection is set to call a phone that has an answering machine, confirm with the user that the answering machine greeting is short enough so that the machine starts recording before the notification message is repeated.

Repeat Notification Option Is Misunderstood

Setting Cisco Unity Connection to repeat notification at a particular interval when there are still new messages can be useful for users who receive a lot of messages but who do not want immediate notification. However, when a user chooses not to have Connection restart notification each time a new message arrives, setting a long interval between repeat notification calls may lead the user to believe that Connection is delaying notification.

To Resolve a Repeat Notification Problem

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 In the Repeat Notification Interval box, set a shorter interval, such as 15 minutes.

Message Notification Is Not Working at All for a User

There are several possible reasons that message notification may not work at all for a user. If SMS notification is not working, see the "SMS Notifications Are Not Working" section on page 11-5. For all other message notifications, use the "Task List for Troubleshooting Non-Functional Message Notifications for a User" to troubleshoot the possible causes.

Task List for Troubleshooting Non-Functional Message Notifications for a User

1. Confirm that message notification is enabled for the correct types of messages. See the "Only Certain Types of Messages Are Set to Trigger Notification" section on page 11-6.
2. Confirm that the message notification phone number includes the access code for an external line if notification is to an external phone. See the "Access Code for an External Line Is Missing" section on page 11-7.
3. Confirm that the notification device is enabled. See the "Notification Number Is Incorrect or the Device Is Disabled or Not Working" section on page 11-7.
4. (Dual phone system integrations only) Confirm that the notification device is assigned to the correct phone system. See the "Notification Device Phone System Assignment Is Incorrect (Dual Phone System Integrations Only)" section on page 11-8.

SMS Notifications Are Not Working

If SMS notifications are not working, check the settings on the Edit SMPP Provider page in Cisco Unity Connection Administration and confirm that the settings match the settings specified by the provider.

If settings on the Edit SMPP Provider page are correct, do the following procedure to turn on macro and micro traces that may help you diagnose the problem.

Turning on Macro and Micro Traces to Diagnose Problems with SMS Notifications

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Diagnostic Tool**.

Step 2 In the right pane of the Cisco Unity Diagnostic Tool, click **Configure Macro Traces**.

Step 3 On the Welcome to the Configure Macro Traces Wizard page, click **Next**.

Step 4 On the Configure Macro Traces page, click **Traces for Other Notification Problems**, and click **Next**.

Step 5 On the Completing the Configure Macro Traces Wizard page, click **Finish**.

Step 6 In the right pane of the Cisco Unity Diagnostic Tool, click **Configure Micro Traces**.

Step 7 On the Welcome to the Configure Micro Traces Wizard page, click **Next**.

Step 8 On the Configure Micro Traces page, expand **Notifier and Notification Devices (Notifier)**, and click **30 SMS Device**.

Step 9 Click **Next**.

Step 10 On the Completing the Configure Micro Traces Wizard page, click **Finish**.

For information on gathering and reviewing the logs, see the "Diagnostic Traces and Event Logs" chapter.

Common error codes and explanations for SMS problems are listed in the following table:

SmppConnect failed	Connection was unable to connect to the SMPP provider.
SmppBindTransmitter failed	Connection was unable to log in to the SMPP provider.
SmppSubmitSm failed	Connection was unable to submit the SMS message to the SMPP provider.

Only Certain Types of Messages Are Set to Trigger Notification

Cisco Unity Connection can be set so that a user is notified only of certain types of messages. For example, if user notification is set up only for the first voice message or only for urgent voice messages, additional voice messages and regular voice messages will not cause Connection to make a notification call.

To Change the Message Types That Trigger Notification Calls

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 In the Notification Event list, verify the selected message types with the user.

Access Code for an External Line Is Missing

To place an external call, a user usually must dial an access code (for example, 9) to get an external line. When the phone system requires an access code, an external message notification phone number set in Cisco Unity Connection must include the access code.

In addition, some phone systems may require a brief pause between dialing the access code and being connected to an external line.

To Verify an Access Code

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 In the Phone Number box, confirm that the correct access code is included before the phone number. If the phone system requires a pause, enter two commas between the access code and the phone number (for example, 9,,5551234).

Notification Number Is Incorrect or the Device Is Disabled or Not Working

The user may have entered a wrong phone number for Cisco Unity Connection to call. Also, when a user disables notification to a phone or pager, Connection will not attempt a notification call to the device regardless of the other notification settings.

To Verify a Device Phone Number and Status

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 In the Device list, click the correct notification device.

Step 5 Confirm that the **Enabled** check box is checked.

Step 6 In the Phone Number box, confirm that the correct access code and phone number are entered for the device.

To Test a Notification Device

Step 1 If the notification device is a cellular phone or pager, ask the user to have it available for the test.

If the notification device is a home phone or another phone away from the office, ask the user to have someone available to answer the phone during the test.

Step 2 Confirm that the notification device is on.

Step 3 Set up a test phone (Phone 1) for single-line testing. Use a line connected to a port that is set to dial out for message notification. For more information, see the "Preparations for Troubleshooting the Phone System" section on page 4-1.

Step 4 On Phone 1, dial the notification number set in Connection for the device.

If the pager is activated or the phone rings, you have confirmed that Connection can call the device.

If the pager is not activated or the phone does not ring, there may be a problem with the device. Consult the documentation from the device manufacturer, or ask the user to obtain a different notification device and repeat the test.

Notification Device Phone System Assignment Is Incorrect (Dual Phone System Integrations Only)

To Verify Notification Device Phone System Assignment

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

Step 2 On the Search Users page, in the Search Results table, click the alias of the applicable user.

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

Step 3 On the Edit User Basics page, on the Edit menu, click **Notification Devices**.

Step 4 Note the phone system that is assigned to the device in the Phone System field at the bottom of the page.

Step 5 In Cisco Unity Connection Administration, expand **Telephony Integration**, then click **Port**.

Step 6 Verify that the phone system assigned to the notification device has at least one port designated for message notification. Correct the port settings if necessary.

Step 7 Click **Save**.

Message Notifications Function Intermittently or Not At All

A possible cause for notification devices (such as phones, pagers, SMTP, and SMS) to function intermittently or not at all is that the schedule for the user is not active during the time in question.

To correct the problem, edit the schedules of the notification devices for the user so that the notification devices are active when the user wants message notifications delivered. The schedules can be edited in the Cisco Personal Communications Assistant.

Notification Devices Added in Cisco Unity Connection Administration Do Not Work

When a notification device is added for a user in Cisco Unity Connection Administration, the device does not have an active schedule. You must log on to the user account in the Cisco Personal Communications Assistant to enter a schedule for notification devices.

Connection Administration does not expose schedules for notification devices.

Non-Delivery Receipts

This chapter contains the following sections:

Troubleshooting Nondelivery Receipts

Determine whether the fault lies with the sender, the recipient, or the Cisco Unity Connection server. To gather more information, send voice messages to the recipient from different users. In addition, send voice messages to different users from the original sender.

Cisco Unity Connection Nondelivery Receipt Status Codes

As you examine a nondelivery receipt (NDR), look for a three-digit code (for example, 4.2.2). Status codes in Cisco Unity Connection have the following meanings:

- 4.2.1—The recipient mailbox has been dismounted.
- 4.2.2—The recipient mailbox is over the allotted quota set by the administrator.
- 4.2.4 —The message was sent to an empty distribution list.
- 4.3.2—The message store where the recipient is located has been dismounted.
- 5.1.1—The recipient mailbox cannot be resolved, possibly because the recipient address does not exist or is not correct.
- 5.2.0—An unknown error condition, and Connection cannot process the message.
- 5.7.2—An error occurred during expansion of a distribution list.

Note The code 2.0.0 indicates success. Delivery and read receipts will contain this status code; NDRs will not.

As you examine an NDR, note that in general, the first decimal place refers to the class of code: 4.x.x is a transient failure and resend attempts may be successful, and 5.x.x is a permanent error. A more detailed analysis and a list of standard errors for SMTP are available in RFC 1893—Enhanced Mail System Status Codes.

CHAPTER 13

Cisco Unity Connection Conversation

This chapter contains the following sections:

Custom Keypad Mapping Does Not Seem to Take Effect

When you use the Custom Key Map tool to customize the key mappings for the Cisco Unity Connection conversation, you must also assign the Custom Keypad Mapping conversation to a user or group of users.

To change the conversation version for a single user, go to the Edit User Basics page. On the Edit menu, click Conversation Settings. To change the conversation style for multiple users, you can use the Bulk Edit utility found in Cisco Unity Tools Depot.

Long Pauses After Listening to the Help Menu

After playing a Help menu, Cisco Unity Connection waits for a key press. Users can press a key for the command they want, or press 0 to hear the Help menu of command options again.

Determining Which WAV File Is Being Played

To determine which WAV file is being played off the hard disk, turn on Phraseserver to Monitor diagnostics in the Cisco Unity Diagnostic Tool, then run Port Status Monitor and make a call to Cisco Unity Connection. Port Status Monitor gives the full path of the WAV files being played. It also provides other technical information that may be helpful in diagnosing conversation issues.

Future Message Delivery

Cisco Unity Connection version 1.x does not support future message delivery.

CHAPTER 14

Voice Recognition

This chapter contains the following sections:

Restarting the CuVrt and Nuance Watcher Daemon Services

For some voice-recognition issues, restarting the CuVrt and Nuance Watcher Daemon services will resolve the problem.

To Restart Services on the Cisco Unity Connection Server

Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Services > Services Control Manager**.

Step 2 In the Services Control Manager window, right-click the CuVrt service and click **Restart**.

Step 3 After the CuVrt service restarts, right-click the Nuance Watcher Daemon service and click **Stop**. Wait about 15 seconds, right-click the Nuance Watcher Daemon service again and click **Start**.

Step 4 After the Nuance Watcher Daemon service restarts, close the Services Control Manager window and wait one to two minutes for the applicable processes to start before accessing voice recognition.

If voice recognition is unavailable or is not recognizing voice commands, check the Windows Task Manager to confirm that the following processes are running (and with the indicated memory allocation):

- Recserver.exe (~ 200,000K)
- Compilation-server (~50,000K)
- Nrcp-server

- Nlm

To Restart Services for a Separate Voice-Recognition Server

Step 1 On the Cisco Unity Connection server, on the Windows Start menu, click **Programs > Administrative Tools > Services > Services Control Manager**.

Step 2 In the Services Control Manager window, right-click the CuVrt service and click **Restart**.

Step 3 On the voice-recognition server, on the Windows Start menu, click **Programs > Administrative Tools > Services > Services Control Manager**.

Step 4 In the Services Control Manager window, right-click the Nuance Watcher Daemon service and click **Restart**.

Step 5 After the Nuance Watcher Daemon service restarts, close the Services Control Manager window and wait one to two minutes for the applicable processes to start before accessing voice recognition.

If voice recognition is unavailable or is not recognizing voice commands, check the Windows Task Manager to confirm that the following processes are running (and with the indicated memory allocation):

- Recserver.exe (~ 200,000K)
- Compilation-server (~50,000K)
- Mrcp-server
- Nlm

Users Hear Touchtone Conversation Instead of Voice-Recognition Conversation

Use the following troubleshooting steps to determine the source of the problem and to correct it:

1. Does this problem occur for one user or for all users configured for voice recognition?
    a. Verify that the class of service (COS) is configured to enable voice recognition. On the Class of Service page, under Licensed Features, check the Allow Users to Access Voice Recognition or Text to Speech for E-Mail check box. Under Features, check the Allow Users to Use Voice Recognition check box.
    b. Verify that the affected user or group of users is associated with the correct COS.
    c. Verify that the phone menu input style is set to voice recognition. The input style can be set either in the Cisco Unity Assistant web tool or in Cisco Unity Connection Administration.
2. Is the voice-recognition server configured correctly?
    a. Verify that the CuVrt service and the Nuance Watcher Daemon service (for both local server and separate voice-recognition server configurations) are running. See the "Restarting the CuVrt and Nuance Watcher Daemon Services" section on page 14-1.
    b. Verify that all processes associated with the Nuance Watcher Daemon service are running optimally. See the "Restarting the CuVrt and Nuance Watcher Daemon Services" section on page 14-1.

3. If you are using a separate voice-recognition server, has the Nuance license file been transferred from the Connection server to the voice-recognition server?
   a. On the Connection server, confirm that the Nuance license file is in the G:\Nuance\V8.5.0\Licenses directory.
   b. On the voice-recognition server, the Nuance license file should also be located in the G:\Nuance\V8.5.0\Licenses directory. If the directory does not exist, copy the Licenses directory from the Connection server to the same location on the voice-recognition server.
4. Is the G.711 codec being used?

   For Cisco Unity Connection 1.1(1), the G.711 Mu-Law audio format is required for Connection voice-recognition features. Voice recognition does not work if the Connection server or the phone system is using G.729a; if the G.729a prompts are installed; or if greetings and names were recorded in an audio format other than G.711 Mu-Law.

   For Cisco Unity Connection 1.2(1), voice recognition does not work if the phone system is using G.729a.

"Voice-Recognition Services Are Not Available" Error Prompt

When a user hears the error prompt "Voice-recognition services are not available. Use the standard touchtones for the duration of the call. Please contact your system administrator if this situation persists," use the following troubleshooting steps:

1. Check the Cisco Unity Connection license on the Connection server and the Nuance license file on the voice-recognition server (if applicable). It may be that all licensed voice-recognition sessions are being used. The Cisco Unity Connection license is located in the Program Files\Cisco Systems\Cisco Unity Connection\Licenses directory. The Nuance license file is located in the Nuance\V8.5.0\Licenses directory.
2. In Cisco Unity Connection Administration, expand System Settings > Voice Recognition Server, and click the name of the voice-recognition server. On the Edit Voice Recognition Server page, check that you have the correct address listed in the IP Address field.

Voice Commands Are Recognized, But User Names Are Not

Restart the CuVrt and Nuance Watcher Daemon services. See the applicable procedure in the "Restarting the CuVrt and Nuance Watcher Daemon Services" section on page 14-1.

Voice Commands Are Not Recognized

1. See the *Cisco Unity Connection User Guide* for a table of preferred voice commands. Although the voice-recognition grammar files contain many synonyms for the preferred commands, it is not possible for them to contain every word or phrase a user might say. For the best performance, encourage users to use the preferred commands.
2. Check the Windows Task Manager to confirm that the following Nuance Watcher Daemon server processes are running (and with indicated memory allocation):
   - Recserver.exe (approximately 200,000K)
   - Compilation-server (approximately 50,000K)

- Mrcp-server
- Nlm

3. Wait for the CuVrt service to update (this can take up to five minutes), or restart CuVrt. See the applicable procedure in the "Restarting the CuVrt and Nuance Watcher Daemon Services" section on page 14-1.
4. Check for the appearance of the following files in the G:\Nuance\V8.5.0\mrcp directory:
   - subscriber.gsl
   - directory.gsl
   - contacts.gsl
5. If it is possible that the voice-recognition system is having trouble understanding how a user name is pronounced, consider adding nicknames or alternate names for the user. Both of these features let you add differing pronunciations for names that are not pronounced the way they would be read. (For example, a user name is Janet but is pronounced Jah-nay. You could add the pronunciation "Jahnay" as an alternate name or nickname.)

   For information on adding nicknames for a user, see the *Cisco Unity Connection System Administration Guide*. See the *Cisco Unity Connection User Moves, Adds, and Changes Guide* for information on adding alternate names for a user. Both guides are available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Users Hear Only Full Menus

This is a known issue for Cisco Unity Connection 1.x. Although Connection users and administrators are able to change the setting for full or brief menus in Cisco Unity Connection Administration and in the Cisco Unity Assistant web tool, the voice-recognition feature is hard-coded to use only full menus. Brief menus will be implemented in a future release.

Users Are Unable to Change Settings by Phone

This is a known issue for Cisco Unity Connection 1.x. Although Connection users may be able to say "Settings" at the Main menu and hear options in phone menu Help, they are unable to change message settings, personal settings, and call transfer settings by phone. The options will be implemented in a future release.

Using Trace Logs in the Cisco Unity Diagnostic Tool

The Cisco Unity Diagnostic Tool (UDT), located in the Cisco Unity Tools Depot, offers diagnostic macro traces and micro traces for help in troubleshooting voice-recognition issues.

Macro Traces

Set the Voice User Interface/Speech Recognition Traces.

Micro Traces

- Conversation Development Environment (CDE)
  - 11 NamedProps Access
  - 16 Call Progress Diags
  - 20 CML Access
  - 22 Speech Recognition Grammar
- Media: Input/Output (MiuIO)
  - 11 Wave Play/Record Success/Failure
  - 25 Media Server
- Subscriber Conversation
  - 10 Call Progress
  - 15 NamedProps Access Failures
  - 26 General Failures
- Phrase Server
  - 15 Speech Recognition

Note See the Cisco Unity Diagnostic Tool Help for more information about using macro and micro traces.

Using Other Logging to Troubleshoot Issues

Errors, warnings, and exception traces captured in event log files can often indicate the source of a problem. In addition, when you report a problem to Cisco TAC, you may be asked to send log files.

When troubleshooting voice-recognition issues, look in the following log file directories for errors and warnings:

- Nuance\Logs
- C:\WINDOWS\System32\Logs

In addition, check the Windows Event Viewer Application log for CuVrt events. Do the following procedure to increase logging verbosity for the CuVrt service.

To Increase Logging Verbosity for the CuVrt Service

Step 1 Open the registry.

Step 2 Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CuVrt. In the Configuration subkey, modify the Event Level value with one of the following values:

Level	Description
0	Set to suppress all logging.
5	Quiet: includes service startup and shutdown and some errors.

Level	Description
10	Standard (default): includes Quiet level logging and all other errors.
15	Verbose: Includes Standard level logging and logging for internal operations.
20	All: Includes Verbose level logging and some registry logging.

Step 3 Restart the CuVrt service:

a. On the Windows Start menu, click **Programs > Administrative Tools > Services > Services Control Manager**.

b. In the Services Control Manager window, right-click the CuVrt service and click **Restart**.

Personal Call Transfer Rules

This chapter contains the following sections:

Cisco Unity Personal Call Transfer Rules Settings Are Unavailable

If a user does not hear the Personal Call Transfer Rules Settings menu in the phone interface or if a user cannot see the Cisco Unity Personal Call Transfer Rules web tool link in the Cisco Personal Communications Assistant, confirm that the user is assigned to a class of service that is enabled for access to the Personal Call Transfer Rules web tool.

In addition, if you are troubleshooting problems with a Connection 1.2 system, do the following procedure to confirm that the value of the Region Restricted Feature licensing option is set to 1. If the value is not 1, you cannot use personal call transfer rules, and you cannot use any languages other than English-United States. To resolve the problem, install a license in which the feature is enabled, and restart Connection. (An additional fee might be required to enable the feature. Contact your Cisco account team to obtain the updated license file.)

To Determine the Value of the Region Restricted Feature Licensing Option

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

Step 2 In the Related Links list, click **View License Usage**.

Step 3 Click **Go**.

Step 4 On the License Count page, confirm that the value of Region Restricted Feature (the tag is called LicRegionIsUnrestricted) is set to **1**.

Step 5 Close the License Count page.

Troubleshooting Destinations

Personal call transfer rules can forward calls to a phone destination, a destination group, or to voice mail. The destination group must contain at least one phone destination, and can also contain SMS and SMTP devices. The destinations in a destination group are tried serially in the priority order in which they are listed until a destination phone is answered or the caller hangs up.

When a user has entered phone numbers for notification devices in the Cisco Unity Assistant web tool, the numbers are displayed on the View Destinations page and can be used as destinations for rules. The notification devices do not need to be enabled. These prepopulated destinations cannot be edited or deleted in the Personal Call Transfer Rules web tool. They can be edited only on the Notification Devices page in the Cisco Unity Assistant.

Note that pager destinations are not supported destinations for rules, and thus are not displayed on the View Destinations page.

Troubleshooting Call Screening or Call Holding Options

If call screening and call holding options are not available in the Personal Call Transfer Rules web tool, confirm that the user belongs to a class of service that allows access to the call screening and/or call holding options.

Note Call holding applies only to calls to primary extensions.

When editing a rule in the Personal Call Transfer Rules web tool, the Screen the Call check box may be grayed out even when the user belongs to a class of service that allows users to access call screening options. If the option is grayed out, do the following procedure to correct the problem.

To Enable the Screen the Call Option in the Personal Call Transfer Rules Web Tool

Step 1 In the Personal Call Transfer Rules web tool, on the Preferences menu, select **Call Holding and Screening**.

Step 2 On the Call Holding and Call Screening Options page, verify that at least one option under the Screen Calls section is enabled.

Troubleshooting the Application of Rules

See the following sections:

- Rules Are Not Applied When a User with Active Rules Receives a Call, page 15-3
- Unexpected Behavior Results When Rules Lack a “From” Condition, page 15-3

- Rules Based on a Meeting Conditions Are Not Applied Correctly, page 15-4
- Rules Based on a Caller or Caller Group Are Not Applied Correctly, page 15-4
- Rules Based on a Time Condition Are Not Applied Correctly, page 15-4

Rules Are Not Applied When a User with Active Rules Receives a Call

There are several reasons that a rule set can fail:

- If the rule set is specified for a day of the week but another rule set is enabled for a date range that includes the current date, the date range rule set takes precedence.
- Transfers to a destination without a complete dialable phone number may fail. If there is no other destination to try, the caller is transferred to voice mail.

Try the following troubleshooting steps:

1. Use the Call Transfer Rule Tester to check the validity of the rule. The test will tell you which rule is currently being invoked. Based on the results, you may want to reprioritize the rules within the rule set.

Note To get results with the Call Transfer Rule Tester, the rule set that contains the rule you are testing must be enabled or active.

2. Confirm that the destinations for the rule set contain dialable phone numbers, including any outdial access codes required by the phone system. See the "Dialable Phone Numbers" section on page 15-3.
3. On the Rules Settings page, confirm that the Disable All Processing of Personal Call Transfer Rules check box is not checked. When checked, the field disables all rule processing.

Dialable Phone Numbers

When adding and editing a personal contact, users can enter a phone number and a dialable phone number for the contact.

Cisco Unity Connection uses the phone number fields—Work Phone, Home Phone, and Mobile Phone—when matching incoming phone calls for personal call transfer rules based on the work, home, or mobile phone number of a personal contact.

The dialable phone number fields—Dialable Work Phone, Dialable Home Phone, and Dialable Mobile Phone—are used by Connection when a user calls a personal contact by using voice commands. (For example, the user says "Call John Smith at work" to place the call.)

To set up dialable numbers, enter the phone number in the applicable dialable number field, beginning with any access code necessary to make an external call (for example, 9). Enter digits 0 through 9. Do not use spaces, dashes, or parentheses between digits. For long-distance numbers, also include 1, the country code, and the area code as applicable.

Unexpected Behavior Results When Rules Lack a "From" Condition

Personal call transfer rules can be created without a "From" condition ("from" or "not from"). When set up this way, the rules are applied to all incoming calls.

Rules Based on a Meeting Conditions Are Not Applied Correctly

When a personal call transfer rule has a condition that is based on a Microsoft Exchange calendar appointment, the rule might not be applied as expected. Calendar information is cached every 30 minutes, so a newly created appointment may not yet be cached.

Try the following troubleshooting steps:

1. Confirm that the WebDav external service is configured properly. In Cisco Unity Connection Administration, expand System Settings > External Services.
2. Confirm that the applicable WebDav service is configured as an External Service Account for the user. In Connection Administration, click Users and search for the user. On the Edit User Basics page, on the Edit menu, click External Service Accounts.

Note See the “Configuring Access to Exchange Calendars and Contacts for Personal Call Transfer Rules” chapter of the *Cisco Unity Connection Installation Guide* for detailed information on setting up external service accounts. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

3. Confirm that the Exchange-server and Connection-server clocks are synchronized to the same time source.

To get around the 30-minute lag for caching appointments, you can force caching of appointments by stopping and restarting the Groupware Server role in the Cisco Unity Connection Server Status utility.

Rules Based on a Caller or Caller Group Are Not Applied Correctly

Phone numbers for primary extension, home phone, work phone, and mobile devices for users; system contacts; and personal contacts must match the incoming caller ID or ANI. Confirm that the phone number of the caller that is specified in Cisco Unity Connection matches the incoming caller ID or ANI.

Rules Based on a Time Condition Are Not Applied Correctly

Confirm that the correct time zone has been selected for the user. In Cisco Unity Connection Administration, click User and search for the user. On the Edit User Basics page, change the selected time zone, as necessary.

Troubleshooting the “Transfer All” Rule

See the following sections:

- Creating a Transfer All Rule, page 15-5
- Transfer All Rule Is Not Applied as Expected, page 15-5

Creating a Transfer All Rule

You cannot create a Transfer All rule in the Personal Call Transfer Rules web tool. The Transfer All rule can be created only by phone. After the rule has been added by phone, it can be edited in the Personal Call Transfer Rules web tools. Both the destination and duration can be changed in the web tool.

Transfer All Rule Is Not Applied as Expected

If the Transfer All rule is not being applied as expected, confirm that the destination number includes any outdial access codes required by the phone system.

Troubleshooting Phone Menu Behavior When Using Personal Call Transfer Rules

See the following sections:

- User Cannot Change Personal Call Transfer Rules by Using Voice Commands, page 15-5
- Phone Menu Options for Personal Call Transfer Rules Vary, page 15-5
- Rule Sets Are Unavailable for Enabling or Disabling by Phone, page 15-5
- Phone Menu Option to Set or Cancel Forwarding All Calls to Cisco Unity Connection Is Unavailable, page 15-6
- Inconsistent Behavior Between Calls Placed Through Cisco Unity Connection and Calls Placed Directly to a User Phone, page 15-6
- Call Looping During Rule Processing, page 15-7

User Cannot Change Personal Call Transfer Rules by Using Voice Commands

The voice-recognition feature does not yet support the Personal Call Transfer Rules phone menu options. If users want to use Personal Call Transfer Rules, they must temporarily switch to the touchtone-key input style. They can temporarily switch to the touchtone-key input style by saying “Touchtone conversation,” or by pressing 9 at the Main menu.

Phone Menu Options for Personal Call Transfer Rules Vary

Users may notice variations in the phone menus for Personal Call Transfer Rules that they hear. Personal Call Transfer Rules phone menu options are built dynamically, and they depend on the existing rule sets and which sets are enabled and active.

Rule Sets Are Unavailable for Enabling or Disabling by Phone

If a rule set does not have a recorded name and there are no Text to Speech sessions available, the rule set will not be available for enabling or disabling by phone. Recording names for rule sets ensures that they will always be available for enabling or disabling by phone.

Phone Menu Option to Set or Cancel Forwarding All Calls to Cisco Unity Connection Is Unavailable

If the phone menu option to set or cancel forwarding all calls to Cisco Unity Connection is unavailable, try the following troubleshooting steps:

1. Confirm that the AXL server settings for the phone system are correct. In Cisco Unity Connection Administration, expand Telephony Integrations > Phone System. On the Phone System Basics page, on the Edit menu, click Cisco Unified CallManager AXL Servers.

Note See the "Managing the Phone System Integrations" chapter of the *Cisco Unity Connection System Administration Guide* for detailed information about AXL server settings. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

2. Check to see if the publisher Cisco Unified CallManager is shut down or if there are network connectivity issues between the Connection and publisher Cisco Unified CallManager servers. Use the Test button on the Edit AXL Server page to test the connection. If the Cisco Unified CallManager publisher database is down, Connection cannot change the Call Forward All (CFA) setting for the phone.

The option to forward all calls to Connection is available only in integrations with Cisco Unified CallManager versions 4.0 and later. The option is not available with earlier versions of Cisco Unified CallManager or with Cisco Unified CallManager Express.

Inconsistent Behavior Between Calls Placed Through Cisco Unity Connection and Calls Placed Directly to a User Phone

Callers may notice inconsistent behavior when calling a user through the Cisco Unity Connection automated attendant and when dialing the user phone directly. Rules are typically applied immediately to calls placed through the automated attendant, while direct calls must wait until the Call Forward No Answer timer for the phone expires before the call is forwarded to Connection. Rules will then be applied.

Use the following troubleshooting steps to provide a consistent caller experience regardless of how a call is placed:

1. To set a user phone to always ring first before rules are applied, turn off the Forward All Calls to Cisco Unity Connection feature by phone. In the Personal Call Transfer Rules web tool, on the Preferences menu, click Rules Settings. On the Rules Settings page, check the Always Ring Primary Extension Before Applying Call Transfer Rules check box.
2. To set user rules for immediate processing, turn on the Forward All Calls to Cisco Unity Connection feature by phone. In the Personal Call Transfer Rules web tool, on the Preferences menu, click Rules Settings. On the Rules Settings page, uncheck the Always Ring Primary Extension Before Applying Call Transfer Rules check box.

Call Looping During Rule Processing

Call looping may occur when calls forwarded by Cisco Unity Connection are forwarded back to Connection and rules are applied again. Callers may experience inconsistent behavior, such as repeated instances of the opening greeting or continuous attempts to reach the same destination.

The following settings can be used to prevent such looping conditions:

- In Cisco Unity Connection Administration, expand Telephony Integrations > Phone System and select the applicable phone system. On the Phone System Basics page, check the Enable for Supervised Transfers check box. The setting causes Connection to detect and terminate call looping conditions so that calls proceed in the desired fashion.
- In the Cisco Unity Personal Call Transfer Rules, on the Destinations > View Destinations page, check the Loop Detection Enabled check box for any phone-type destinations to help eliminate call-looping problems where Connection forwards calls to the mobile phone of the user, and the mobile phone consequently forwards calls back to Connection. When this setting is enabled, Connection will either transfer the call to the next assigned device (if the user has created a destination group) or transfer the call to voice mail if there are no additional destinations defined.
- *(For integrations with Cisco Unified CallManager only)* Allow Connection to maintain control of calls by setting the value in the Rings to Wait field for rule destinations to be less than the value in the Cisco Unified CallManager Forward No Answer Timer field. The Cisco Unified CallManager Forward No Answer Timer value defaults to 12 seconds. One ring occurs about every 3 seconds. Thus, setting the Rings to Wait value for Connection destinations to 3 will allow Connection to maintain control of the call. The supervised transfer initiated by Connection will pull back the call before the loop begins and attempt to transfer the call to the next destination or to voice mail, as applicable.

Diagnostics for Personal Call Transfer Rules

The following micro traces can be enabled in the Cisco Unity Diagnostic Tool (UDT) to debug the various rule components:

- Rules Engine—Used in rule processing during calls to a rules-enabled user to determine the applicable rule. Also used in determining the applicable rule when using the Rules Tester.
- Routing Rules Conversation—Used when a rules-enabled user receives a call and while transferring calls between destinations.
- Subscriber Conversations—Used when configuring personal call transfer rules settings by phone.
- Conversation Development Environment (CDE)—Used in rules-related conversations.
- PHTransfer Conversations (ConvPH Transfer)—Used in rule processing during calls to a rules-enabled user.

In addition, the following diagnostic micro traces for the supporting components can be enabled, if necessary:

- PHGreeting Conversation (ConvPH Greeting)—Used in rule processing during calls to a rules-enabled user when transferring to voice mail.
- Client Data Library (CDL)—Used in rules-related conversations.
- GAL: Cache, GAL: Data, GAL: Distributed Authoring and Versioning, GAL: SQL, GAL:Test, and Groupware Access Library (CuGAL)—WebDav logging used in rule processing with meeting condition and for importing personal contacts.

- Media: Call (MiuCall) and Media: General (MIU General)—Used in rule processing during calls to a rules-enabled user.
- Phrase Server (PhraseServer)—Used in rules-related conversations to play prompts.
- Notifier and Notification Devices (Notifier)—Used in rule processing when sending SMTP and SMS messages.
- Text to Speech—Used in rule-settings conversation.

Performance Counters for Personal Call Transfer Rules

The following performance counters are provided for the Personal Call Transfer Rules feature under the Connection: Transfer Rules performance object:

- Subscriber Reached—Number of times a user was reached while applying personal call transfer rules.
- Transfer Failed—Number of times a transfer to a destination failed while applying personal call transfer rules.
- Voice Mail Reached—Number of times voice mail was reached while applying personal call transfer rules.
- Applicable Rule Found—Call resulted in rule processing, and an applicable rule was found.
- Destinations Tried—Number of destinations tried while applying personal call transfer rules.
- Rules Evaluated—Number of rules evaluated during rule processing in a call.
- PCTR Calls—Call is subject to personal call transfer rules processing: user is assigned to a class of service that has the Personal Call Transfer Rules feature enabled; user is associated with a Cisco Unified CallManager phone system; and user has not disabled personal call transfer rules.

Cisco Personal Communications Assistant

The Cisco Personal Communications Assistant (PCA) is the portal that provides access to the Cisco Unity Connection web tools for users to manage messages and personal preferences in Cisco Unity Connection. The Connection web tools include the Cisco Unity Assistant, the Cisco Unity Inbox, and the Cisco Unity Personal Call Transfer Rules. The Cisco PCA is installed on the Connection server during installation.

See the following sections:

- About Cisco PCA Logging, page 16-1
- Troubleshooting the Cisco PCA and Its Components, page 16-1
- Cisco PCA Error Messages, page 16-2
- Troubleshooting Whether Services Are Started, page 16-4

About Cisco PCA Logging

Errors, warnings, and exception traces captured in log files can often indicate the source of a problem. In addition, when you report a problem to Cisco TAC, you may be asked to send log files.

Each day, the Cisco PCA logs events in the following files in the %CU_HOME%\logs directory:

- The ciscopca_log.txt.<date> file contains a daily archive of system level logs.
- The ciscopca_diags_log.txt.<date> file contains a daily archive of application logs.
- The ciscopca_event_log.txt.<date> file contains a daily archive of application error logs.

Troubleshooting the Cisco PCA and Its Components

When the Cisco Personal Communications Assistant fails to operate properly, do the following tasks in the order presented. If you cannot resolve the problem and plan to report the problem to Cisco TAC, you will be asked to provide information about your system and about the problem. See the "Reporting Problems to Cisco TAC" section on page 1-10 for details.

1. If there is an error message associated with the problem, review the "Cisco PCA Error Messages" section on page 16-2, and then return to this section as needed.

2. Review the "Users Cannot Access Cisco Personal Communications Assistant Pages" section on page 6-2 to consider the most common reasons why users cannot access the Cisco PCA pages, including use of an incorrect URL, incorrect browser settings, and presence of unsupported software installed on the workstation.
3. If users cannot browse to the Cisco PCA website at all, experience incomplete or blank Cisco PCA pages, or have trouble accessing the Cisco PCA applications, see the "User and Administrator Access" chapter for the applicable troubleshooting procedures.
4. If the problem is that Media Master control bar does not show up correctly or at all, see the "Media Master" chapter.
5. Confirm that the %CU_JAVA_HOME% directory exists on the Cisco Unity Connection server, and that it contains a Bin directory. If this directory is missing, the tomcat service will fail to start and other Cisco Unity Connection components will fail to operate. The only corrective action is to reinstall Connection. See the *Cisco Unity Connection Installation Guide* for procedures and information (the guide is available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html).
6. Confirm that the %CATALINA_HOME% directory exists on the Cisco Unity Connection server and that it contains the webapps\ciscopca directory. If this directory is missing, the only corrective action is to reinstall Connection. See the *Cisco Unity Connection Installation Guide* for procedures and information.
7. Confirm that the Tomcat service is installed and that the service has started. See the "Verifying That the Tomcat Service Is Installed and Started" section on page 16-4.

Cisco PCA Error Messages

In addition to browser error messages (such as "File not found" or "Unauthorized access"), users may see Cisco PCA-specific error messages, Java plugin error messages, and Tomcat error messages when logging on to the Cisco PCA, or when using the Cisco Unity Assistant, the Cisco Unity Inbox, or Cisco Unity Personal Call Transfer Rules.

The four types of error messages that users may encounter are described in the following table:

Browser error messages	Browser error messages may indicate that the Cisco PCA failed to install, the user does not have network access to the Cisco Unity Connection server, the browser is not configured correctly, or the user does not have the required security certificate installed (if the Cisco PCA uses SSL connections).
Cisco PCA-specific error messages	Cisco PCA-specific error messages are displayed on the Log On page or another Cisco PCA page, and typically indicate problems with user credentials or actions within the Cisco PCA.
Java Plugin error messages	Java Plugin-specific error or warning messages are pop-up alerts that occur on pages that load the Java plugin to integrate the Media Master control bar in a web page. These messages typically appear the first time that the Java plugin is loaded when you navigate to a page that contains the Media Master control bar.

Tomcat error messages	Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the Cisco Unity Connection server. A Tomcat error message usually lists the sequence of application errors, starting from the least-likely exception to the root exception. Each exception is followed by a description of what the Tomcat service was attempting to do when the error occurred, and for some exceptions, a message explaining the error is also offered. The "Exception" and "Root Cause" sections in the error message may offer additional information about the problem.

See the following sections for information about these specific error messages:

- Error Message: "Access Denied – Account Is Locked", page 16-3
- Error Message: "Apache Tomcat/<Version> – HTTP Status 500 – Internal Server Error", page 16-3
- Error Message: "Site Is Unavailable", page 16-4
- Error Message: "This Is Not a Cisco Unity Connection Account. Try Logging On With a Different Account. If You Still Cannot Log On, Contact Your Cisco Unity Connection Administrator", page 16-4

Error Message: "Access Denied – Account Is Locked"

When users encounter the error message "Access denied – account is locked," it is possible that the user exceeded the number of failed logon attempts that is allowed. (This limit is set on the System Settings > Authentication Rules page in Cisco Unity Connection Administration.) It may also be possible that the user forgot his or her credentials, or an unauthorized user attempted to gain access.

Use the following task list to determine the source of the problem and correct it.

1. To verify that the account is locked, in Cisco Unity Connection Administration, go to the Users > Edit Password Settings page for the individual user, and select Web Application from the Choose Password menu. Under Web Applications Password Settings, you can verify the status of the user credentials to determine if the password was locked by an administrator, if there were several failed logon attempts, and if the password was locked after an excessive number of failed logon attempts.
2. To unlock the user account, in Cisco Unity Connection Administration, go to the Users > Edit Password Settings page for the individual user, and select Web Application from the Choose Password menu. Under Web Applications Password Settings, click Unlock Password.

Error Message: "Apache Tomcat/<Version> – HTTP Status 500 – Internal Server Error"

File corruption at the time of installation or a Tomcat memory corruption can cause users to encounter the error message "Apache Tomcat/<version> – HTTP status 500 – internal server error." To confirm that this is the cause of the problem, check the Tomcat error page for the indicated root cause for the exception. If an exception message similar to the one below exists, there is a file or memory corruption:

```
java.lang.ClassFormatError: <classpath>/<classname> (Illegal constant pool index)
```

In addition, check the Cisco PCA logs as described in "About Cisco PCA Logging" section on page 16-1, as the logs may also indicate a memory leak.

Error Message: “Site Is Unavailable”

There are several possible reasons why users encounter the error message “Site is unavailable.” Use the following task list to determine and correct the source of the problem.

1. Verify that the Cisco Unity Connection Web Services server role is started and running. See the “Verifying That the World Wide Web Publishing Service Is Started” section on page 16-5.
2. Verify that the Apache Tomcat service is installed and can be started from the Windows Services tool. See “Verifying That the Tomcat Service Is Installed and Started” section on page 16-4.

Error Message: “This Is Not a Cisco Unity Connection Account. Try Logging On With a Different Account. If You Still Cannot Log On, Contact Your Cisco Unity Connection Administrator”

If a user with valid credentials but who does not have an associated Cisco Unity Connection mailbox attempts to log on to the Cisco PCA, the user will receive the error “This is not a Cisco Unity Connection account. Try logging on with a different account. If you still cannot log on, contact your Cisco Unity Connection Administrator.”

To correct the problem, create an account with a mailbox for the user. As a best practice, we recommend that Cisco Unity Connection administrators do not use the same user account to log on to Cisco Unity Connection Administration that they use to log on to the Cisco PCA to manage their own Cisco Unity Connection account.

Troubleshooting Whether Services Are Started

See the following sections:

- Verifying That the Tomcat Service Is Installed and Started, page 16-4
- Verifying That the World Wide Web Publishing Service Is Started, page 16-5

Verifying That the Tomcat Service Is Installed and Started

Do the following procedure to verify that the Tomcat service is installed and started.

To Verify That the Tomcat Service Is Installed and Started

Step 1 On the Cisco Unity Connection server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.

Step 2 In the right pane, locate Apache Tomcat and verify that its status is **Started** and its Startup Type is **Automatic**.

If the Apache Tomcat service is not listed in the services manager, it is likely that the Cisco Unity Connection server installation failed, or the Connection server failed to install and register the Apache Tomcat service. To correct the problem, see the *Cisco Unity Connection Installation Guide*, available at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Caution If the Apache Tomcat service is listed in the services manager, but is not started, do not start the Apache Tomcat service from the services manager. Instead, from the service manager confirm that the startuptype is **Automatic** (recommended) or **Manual**, and then start the Web Services server roles from the Cisco Unity Connection Server Status Tool.

Verifying That the World Wide Web Publishing Service Is Started

Do the following procedure to verify that the World Wide Web Publishing service is installed and started.

To Verify That the World Wide Web Publishing Service Is Installed and Started

Step 1 On the Cisco Unity Connection server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.

Step 2 In the right pane, locate World Wide Web Publishing and verify that its status is **Started** and its Startup Type is **Automatic**.

If the World Wide Web Publishing service is not listed in the services manager, it is possible that IIS was not installed correctly. To correct the problem, you will need to repair the IIS installation.

If the World Wide Web Publishing service is listed in the services manager but is not started, right-click it, and click **Start**.

CHAPTER 17

Media Master

This chapter contains the following sections:

- Understanding Why the Media Master Control Bar May Not Display or Function Correctly in Cisco Unity Connection Applications, page 17-1
- Understanding How the Phone Device Works in the Media Master Control Bar, page 17-2
- Understanding How the Local Device Works in the Media Master Control Bar, page 17-4

Understanding Why the Media Master Control Bar May Not Display or Function Correctly in Cisco Unity Connection Applications

The Media Master control bar may not display or function correctly depending on the operating system and/or browser software installed on the client workstation. See the sections below for information on known browser issues:

- Apple Safari, page 17-2
- Microsoft Internet Explorer, page 17-2
- Mozilla Firefox, page 17-2

See the “Configuring an Internet Browser to Access the Cisco PCA” section in the “Setting Up Access to the Cisco Personal Communications Assistant” chapter of the *Cisco Unity Connection User Setup Guide* for information on how to set up Internet browser(s) on each user workstation to use the Cisco PCA and the web tools. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

For information on the supported version combinations of Cisco Unity Connection and the software installed on user workstations, see the *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations* available at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.

Also consider that some security and VPN software that is installed on the user workstations can cause problems for the Media Master control bar applet. In particular, software that offers personal firewalls can be problematic. If this is the case, work with the software vendor to determine a configuration that will allow the Media Master control bar applet to contact the Cisco Unity Connection server, or disable or remove the conflicting security and VPN software from the user client workstation.

Apple Safari

Apple Safari users are prompted to open a download site to obtain the Java plugin installer the first time they browse to a Cisco PCA page that should contain a Media Master control bar. After the desired version is downloaded and installed, users may have to log off of the Cisco PCA, and close and restart the browser software for the plugin to load properly.

Microsoft Internet Explorer

Microsoft Internet Explorer users are prompted to install the Java plugin the first time that they browse to a Cisco PCA page that should contain a Media Master control bar. Users must have local rights to their workstation in order for the Java plugin to install properly. In addition, the user might have to restart the browser for the newly installed plugin to load. If users choose not to install the Java plugin, they will see a message in place of the Media Master Control Bar stating that support for “application/x-java-applet” is disabled, and pages containing the Media Master Control Bar will pop up one or more alert messages.

Because the Media Master control bar is a Java Applet, and because all Internet Explorer plugins are wrapped into an ActiveX control, users must configure their browsers to download and run ActiveX controls to support automatic plugin installation and to ensure that the Media Master control bar works correctly.

Mozilla Firefox

Mozilla Firefox users are prompted to open a download site to obtain the Java plugin installer the first time that they browse to a Cisco PCA page that should contain a Media Master control bar. After the desired version is downloaded and installed, users may have to log off of the Cisco PCA, and close and restart the browser software for the plugin to load properly.

For users using Mozilla Firefox on Red Hat Linux workstations, the J2SE software uses the Advanced Linux Sound Architecture (ALSA) driver to access system sound devices and control playback and recording functionality. Depending on the sound card, playback and recording capabilities may be limited.

Understanding How the Phone Device Works in the Media Master Control Bar

The Media Master control bar supports using your phone as a playback and recording device. The phone device is always available to users. Users can configure the phone device by selecting “Playback & Recording” from the Options menu on the Media Master control bar. From the Playback & Recording Options window, users can configure the active phone number for the phone device (the default value is the primary Connection extension of the user).

Note See the “The Tools You Use” chapter in the *Cisco Unity Connection User Guide* for more information on configuring the Media Master control bar. The guide is available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.

The phone device sends requests over the network to the Cisco Unity Connection server to call the active phone number. When the phone answers, the phone device proceeds with either playing back or recording the voice recording. The call can fail for these reasons:

- Either no active phone number value is defined, or it is defined incorrectly.
- The phone switch to which the user is assigned does not have any TRAP ports enabled.
- All TRAP-capable ports on the switch are busy.
- Security settings or software prevent the Media Master control bar from contacting the Connection server.

Note that using the phone device is the primary way to listen to or to record secure messages, and to review voice recordings in formats that are not supported by the Media Master control bar local device.

Troubleshooting Problems with the Phone Device Ringing the Phone for Playback or Recording of a Voice Message

Use the troubleshooting information in this section if the phone device either does not ring the phone, or rings the phone only once for playback or recording of voice messages.

See the following possible causes of this issue:

- Phone Numbers of Different Lengths Are Configured on the Phone Switch, Causing the Switch to Wait for Additional Digits, page 17-3
- Phone Number Dialed by the Media Master Control Bar Is Not the Expected Number, page 17-3
- Media Master Control Bar Software Is Not Updated After a Cisco Unity Connection Server or Hotfix Upgrade, page 17-3

Phone Numbers of Different Lengths Are Configured on the Phone Switch, Causing the Switch to Wait for Additional Digits

If your site uses phone numbers that vary in length—for example, some users have five-digit numbers and others have four-digit numbers—this can cause a slight delay (of approximately two seconds) before the call is connected.

The reason for this delay is that there is a conflict with the number of rings that Connection should wait before determining that the phone number did not answer.

Phone Number Dialed by the Media Master Control Bar Is Not the Expected Number

Verify that the active phone number specified in the Media Master control bar is correct. To do this, check the Active Phone Number value for the Primary Extension or Other Number in the Playback & Recording Options window for the Media Master control bar. See the "The Tools You Use" chapter in the *Cisco Unity Connection User Guide* for more information on configuring the Media Master control bar. The guide is available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.

Media Master Control Bar Software Is Not Updated After a Cisco Unity Connection Server or Hotfix Upgrade

If the Media Master control bar software is not updated, this is usually caused by the Java plugin not reloading the Media Master control bar files from Cisco Unity Connection, and instead using the locally-cached versions of the files. If this happens, you can manually update the Media Master control bar software by doing the following procedure.

To Update the Media Master Control Bar Software

Step 1 Close all browser windows.

Step 2 Depending on your operating system, do one of the following:

- For Windows 2000 and later, start the Java control panel by clicking **Start > Settings > Control Panel > Java**.
- For Red Hat Linux and Mac OSX, start the Java control panel found in $JAVA_HOME\bin\ControlPanel.

Step 3 On the General page, under Temporary Internet Files, click **Delete Files**.

This clears the cached files. The Media Master control bar resource files will be downloaded the next time you visit a Cisco PCA or Cisco Unity Connection Administration page that contains the Media Master control bar.

Understanding How the Local Device Works in the Media Master Control Bar

The Media Master control bar supports using your computer (or local device) as a playback and recording device. The local, or "Use Computer" device option in the Media Master control bar interface is offered on most systems that have compatible sound systems and drivers. See the "Setting Up Playback and Recording Devices for the Media Master" chapter in *Cisco Unity Connection User Setup Guide* for more information on Media Master control bar playback and recording capabilities. The guide is available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Local playback of a voice recording is done by streaming the voice recording from the Cisco Unity Connection server the first time it is played. Then, after enough data has been received, the recording format is analyzed by the system to determine whether the Media Master control bar can play the voice recording locally. If the recording cannot be played locally, an error message is shown. The default playback device for the system is used for playing back voice recordings.

Local recording of a voice recording is done (when supported) from the default system microphone device.

APPENDIX A

Using Microsoft Remote Desktop to Administer the Cisco Unity Connection Server

Limitations

Microsoft Remote Desktop is an application that can be used to remotely access the Cisco Unity Connection server. Remote Desktop is automatically installed but not enabled by the Cisco Platform Configuration disk. Note the following limitations with using Remote Desktop:

- You cannot access the Cisco Unity Connection Server Status utility.
- You cannot see any Cisco Security Agent for Cisco Unity pop-up notifications. This can cause problems when you are installing applications or doing file modifications.
- Do not remotely access the Connection server by using a remote desktop "console" session. Running Remote Desktop in console mode remaps the WAV driver to the connecting client, which will cause the telephony integration with your phone system to fail. This will manifest as dropped calls on the server.
- Remote Desktop allows multiple remote sessions logged on to the system at one time. This should be avoided by always logging off when using Remote Desktop or forcing users to log off when a session ends. See the "To Log Off When Using Microsoft Remote Desktop" procedure on page A-1.

In general, VNC is a better application to use for remotely maintaining Connection. It does not have any limitations. However there is a slight increase in CPU utilization during a VNC session with a remote client running.

To avoid potential service performance problems, avoid using any remote access program while the Connection server is under a medium to heavy load.

To Log Off When Using Microsoft Remote Desktop

Step 1 On the Cisco Unity Connection server, on the Windows Start menu, click **Administrative Tools > Terminal Services Configuration**.

Step 2 In the left tree control, click **Connections**.

Step 3 In the right window, double-click **RDP-Tcp**.

Step 4 In the RDP-Tcp Properties dialog box, on the Session tab, set the When Session Limit Is Reached or Connection Is Broken field to **End Session**.

Step 5 On the Network Adaptor tab, set the Maximum Connections field to **1**.

INDEX