



Cisco Unity Troubleshooting Guide (With IBM Lotus Domino)

Release 4.0(3)
September 5, 2003

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4761-01



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

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

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

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

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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

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



Preface i-i

- Audience i-i
- Organization i-i
- Document Conventions i-i
- Cisco Unity Documentation i-ii
- Obtaining Documentation i-ii
 - Cisco.com i-ii
 - Documentation CD-ROM i-iii
 - Ordering Documentation i-iii
 - Documentation Feedback i-iii
- Obtaining Technical Assistance i-iii
 - Cisco TAC Website i-iv
 - Opening a TAC Case i-iv
 - TAC Case Priority Definitions i-iv
- Obtaining Additional Publications and Information i-v

CHAPTER 1

Introduction 1-1

- Preparations for Troubleshooting the Phone System 1-1
 - Setting Up For a Diagnostic Test (Cisco CallManager or SIP Integrations Only) 1-1
 - Setting Up for a Single-Line Test (Circuit-Switched Phone System Integrations Only) 1-2
- Reporting Problems to Cisco TAC 1-3
 - System Information 1-4
 - Problem Description 1-6

CHAPTER 2

Logs and Traces 2-1

- Cisco Unity and Third-Party Logs and Traces 2-1
 - Dr. Watson Logs 2-1
 - Event Log Traces 2-2
 - Miu Diagnostics 2-2
 - TSP Traces 2-4
- Domino Directory Monitor Diagnostic Traces 2-5

CHAPTER 3

Internal and External Calls 3-1

- About Problems with Internal and External Calls 3-1
- Cisco Unity Is Not Answering Any Internal and/or External Calls 3-1
 - Confirming the Phone System Settings 3-2
 - Confirming That a COM Port Is Available to Cisco Unity (Serial or SMDI Integrations Only) 3-2
 - Enabling the ForceGlobalAcmThreadSafety Registry Setting When Corruption in Windows ACM Causes Callers to Hear Reorder Tone or Dead Air Shortly After Cisco Unity Startup 3-3
 - Confirming That the Phone System Generates a Ring Signal (Circuit-Switched Systems Only) 3-5
- Cisco Unity Is Not Answering Some Internal or External Calls 3-5
 - Confirming Hunt Groups 3-6
 - Confirming Routing Rules 3-7
 - Confirming Voice Messaging Port Licensing 3-8
 - Confirming Voice Messaging Port Settings 3-8
 - Confirming Phone Lines and Voice Cards 3-9

CHAPTER 4

Call Transfers 4-1

- About Call Transfer Problems 4-1
- Calls Are Not Transferred to the Correct Greeting 4-1
 - Confirming That the Forward Timer in the Phone System Is in Synch with the Rings to Wait For Setting in Cisco Unity 4-2
 - Confirming That the Phone System Programming Enables Callers to Hear the Subscriber Personal Greeting 4-3
- Subscriber Hears a Reorder Tone When Answering a Call from Cisco Unity 4-3

CHAPTER 5

Messages 5-1

- About Problems with Messages 5-1
- Messages Appear to Be Delayed 5-1
 - Subscriber Misunderstandings 5-2
 - Cisco Unity Domino Server Is Down or Is Disconnected 5-2
- Some Messages Seem to Disappear 5-2
 - Undeliverable Messages Have Not Been Forwarded to Recipients 5-3
 - Subscribers Assigned to Cisco Unity Entities Were Deleted and No Replacements Were Assigned 5-3
- Cisco Unity Stops Recording Before a Caller Has Finished Leaving a Message 5-3
 - Dialogic Quiet Parameter Is Incorrect 5-4
 - Cisco Unity, the Phone System, or the Central Office Disconnected the Call 5-4
- Dial Tone or Reorder Tone Is Present at the End of a Message 5-5

CHAPTER 6**Audio Quality 6-1**

- About Audio Quality Problems 6-1
- Audio Quality Problems in Cisco Unity 6-1
- Set Volume Level Utility 6-2
- Advanced Audio Quality Troubleshooting in Cisco Unity 6-3
- Set Record Format Utility 6-5
- Cisco Unity-CM TSP Wave Gain 6-6
- Automatic Gain Control 6-7
 - Cisco Unity Automatic Gain Control and Registry Settings 6-7
 - Dialogic Voice Card Automatic Gain Control and Registry Settings 6-9
- Comfort Noise 6-10
- Audio Troubleshooting Utilities 6-11
 - AudioStat 6-11
 - CAP Ripper 6-13
 - RTP Parser 6-14

CHAPTER 7**Message Waiting Indicators (MWIs) 7-1**

- How MWIs Function 7-1
- Troubleshooting MWIs When They Do Not Turn On or Off 7-4
 - Miu Component 7-4
 - Notifier and Notifier Queue Components 7-8
- Troubleshooting MWIs When They Are Delayed Turning On and Off 7-10
 - Cisco Unity Domino Server Is Down or Is Disconnected 7-10
 - Ports Are Too Busy to Turn MWIs On and Off Promptly 7-10
 - Not Enough Ports Are Set for MWIs 7-11
 - Calls Are Sent to Cisco Unity Ports That Set MWIs but Do Not Answer Calls 7-11
- Troubleshooting MWIs When They Sometimes Do Not Turn Off 7-12
 - MWIs Have Lost Synchronization 7-12
- Additional References 7-12

CHAPTER 8**Message Notification Calls 8-1**

- About Problems with Message Notification Calls 8-1
- Message Notification Is Slow for Multiple Subscribers 8-1
 - Ports Are Too Busy to Make Notification Calls Promptly 8-2
 - Not Enough Ports Are Set for Message Notification Only 8-2
 - Confirming That the Phone System Sends Calls to the Ports Set to Answer Calls 8-2
 - Cisco Unity Domino Server Is Down or Is Disconnected 8-3

- Message Notification Is Slow for a Subscriber 8-3
 - Message Notification Setup Is Inadequate 8-3
 - Notification Attempts Are Missed 8-4
 - Repeat Notification Option Is Misunderstood 8-4
- Message Notification Calls Are Not Made to Any External Numbers 8-5
- Message Notification Is Not Working at All for a Subscriber 8-5
 - Only Certain Types of Messages Are Set to Trigger Notification 8-6
 - Access Code for an External Line Is Missing 8-6
 - Notification Number Is Incorrect or the Device Is Disabled or Not Working 8-6
 - Notification Device Phone System Assignment Is Incorrect (Dual Phone System Integrations Only) 8-7

CHAPTER 9

Hardware 9-1

- About Problems with Hardware 9-1
- Network Interface Card Problems 9-1
 - Cisco Unity Plays System Prompts but Does Not Transmit Voice 9-1
 - CreateUser Errors Occur During a False Network Disconnect 9-2
- Voice Cards Incorrectly Reported As New Hardware or Missing Drivers 9-3

CHAPTER 10

Error Messages 10-1

- About Error Messages 10-1
- Startup Error Messages 10-1
 - Cisco Unity Fails to Start 10-2
- Cisco Unity Administrator Browser Error Messages and Windows Error Messages 10-3
- E-Mail and Voice Error Messages 10-5

CHAPTER 11

Third-Party Fax Integration 11-1

- About Problems With a Third-Party Fax Integration 11-1
 - A Subscriber Cannot Send or Receive Faxes 11-1
 - A Subscriber Did Not Receive an Attached File Delivered to a Fax Machine 11-1
 - A Fax Did Not Arrive at the Destination 11-2

CHAPTER 12

Utilities 12-1

- Tools Depot 12-1
- Integration Monitor 12-1
 - Values Displayed in the Integration Monitor 12-2
 - Integration Monitor Display Options 12-3
 - Frequently Asked Questions About the Integration Monitor 12-4

Integration Monitor Troubleshooting	12-4
Learn Tones	12-5
Tones Defined in the Switch Configuration File	12-5
Switch Configuration File Location	12-6
Running the Learn Tones Utility	12-6
Troubleshooting the Learn Tones Utility	12-9
Call Viewer	12-10
Cisco Unity Diagnostic Tool	12-11
Advanced Settings Tool	12-13
Universal Dialogic Diagnostics Utility	12-14
Port Status Monitor	12-15

CHAPTER 13**Subscriber and Administrator Access 13-1**

About Access Problems	13-1
Subscribers Logging On to Cisco Unity Hear the Opening Greeting Instead of the Subscriber Conversation	13-2
Cisco Unity Does Not Respond to Touchtones	13-2
DTMF Signal Is Not Being Sent (Cisco CallManager Only)	13-2
DTMF Signal Is Not Being Sent (Circuit-Switched Phone Systems Only)	13-3
DTMF Values in Cisco Unity Are Inconsistent with the Values in the Phone System (Circuit-Switched Phone Systems Only)	13-4
Cisco Personal Communications Assistant Pages Cannot Be Opened or Have Been Defaced	13-4
Subscribers Cannot Access Cisco Personal Communications Assistant Pages	13-5
Subscribers Cannot Access the Cisco Unity Assistant from the Cisco PCA	13-6
Subscribers Cannot Save Changes on Pages in the Cisco Unity Assistant	13-6
No Sounds Play on the Multimedia System After Installing the Cisco CallManager Software	13-7
Subscribers Cannot Be Located in a New or Updated Directory Handler	13-7
Cisco Unity Tray Icon Is Missing from the Status Bar	13-8
Cisco Unity Administrator or Status Monitor Pages Cannot Be Opened or Have Been Defaced	13-8
Cisco Unity Administrator Page Cannot Be Accessed After an Upgrade	13-8
Virus Incidents and Hacker Attacks	13-9

CHAPTER 14**Reports 14-1**

About Problems With Reports	14-1
A Requested Report Was Not Generated	14-1
Report Notification Not Generated	14-2

CHAPTER 15

Cisco Personal Communications Assistant 15-1

- About Cisco PCA Installation, Repair, and Removal 15-1
- About Cisco PCA Logging 15-1
- Procedures for Troubleshooting the Cisco PCA and Its Components 15-2
 - Restoring the Cisco PCA 15-2
 - Verifying That the Tomcat Service Is Installed and Started 15-3
 - Verifying That the World Wide Web Publishing Service Is Started 15-3
 - Verifying That IIS and the Cisco PCA Components Are Configured Correctly 15-3
 - Verifying That the IIS and Tomcat Integration Is Configured Correctly 15-6
 - Removing the Cisco PCA 15-7
- Cisco PCA Error Messages 15-8
- Procedures for Troubleshooting the Media Master Control Bar 15-9

APPENDIX A

Cisco Unity Services and Their Functions A-1

- Behavior of Cisco Unity Services in a Configuration with Domino A-2

INDEX



Preface

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

Audience

The *Cisco Unity Troubleshooting Guide* is written for technicians and information systems professionals who configure and manage Cisco Unity. This guide requires knowledge of and access to the phone system, the network, and the voice messaging system.

Organization

The *Cisco Unity Troubleshooting Guide* is divided into sections relating to general problem areas.

Each section addresses a specific problem, which is listed in the section title. The section contains possible causes, and procedures with which you can determine if a possible cause applies to your situation, and resolve the problem.

When the expected result is achieved during a procedure, continue with the next step when applicable, or continue with the next possible cause within the section.

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

Document Conventions

Table 1 *Cisco Unity Troubleshooting Guide Conventions*

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none">• Key and button names. (Example: Click OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)

Table 1 Cisco Unity Troubleshooting Guide Conventions

Convention	Description
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter ping <IP address> .)
- (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: <ul style="list-style-type: none"> On menus. (Example: On the Windows Start menu, click Settings > Control Panel > Phone and Modem Options.) In the navigation bar of the Cisco Unity Administrator. (Example: Go to the System > Configuration > Settings page.)

The *Cisco Unity Troubleshooting Guide* also uses the following conventions:

**Note**

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

**Caution**

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

Cisco Unity Documentation

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

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

You can send your comments in e-mail to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco TAC Website

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

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

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

Opening a TAC Case

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

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

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

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

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

Obtaining Additional Publications and Information

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

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



Introduction

In this chapter you will find basic information that will help you prepare for troubleshooting Cisco Unity. See the following sections:

- [Preparations for Troubleshooting the Phone System, page 1-1](#)—This section includes instructions for setting up for a diagnostic test.
- [Reporting Problems to Cisco TAC, page 1-3](#)—This section explains what information you will need to interact with the Cisco Technical Assistance Center (TAC).

Preparations for Troubleshooting the Phone System

Problems with external and internal calls, message notification calls, and message waiting indicators can be caused by the phone system, by Cisco Unity, 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 Cisco Unity 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 procedures in this section.

Depending on your phone system, do one of the following to set up for troubleshooting:

- [Setting Up For a Diagnostic Test \(Cisco CallManager or SIP Integrations Only\), page 1-1](#)
- [Setting Up for a Single-Line Test \(Circuit-Switched Phone System Integrations Only\), page 1-2](#)

Setting Up For a Diagnostic Test (Cisco CallManager or SIP Integrations Only)

To do diagnostic tests you need three test extensions. Phone 1 is assigned to a test subscriber. Phones 2 and 3 are set up only in Cisco CallManager and do not need to have a Cisco Unity subscriber assigned. All three extensions must be in the same calling search space as Cisco Unity.

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 is connected to.
- Step 2** Set Phone 1 to forward calls to the Cisco Unity pilot number when calls are not answered or when the called extension is busy.

- Step 3** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page for the test subscriber.
- Step 4** In the Extension field, enter the extension of Phone 1.
- Step 5** Click the **Save** icon.
- Step 6** In the navigation bar, click **Call Transfer** to go to the Subscribers > Subscribers > Call Transfer page for the test subscriber.
- Step 7** Under Transfer Incoming Calls, click **Yes, Ring Subscriber's Extension**, and confirm that the extension number is for Phone 1.
- Step 8** Under Transfer Type, click **Release to Switch**.
- Step 9** Click the **Save** icon.
- Step 10** Click **Messages** for the test subscriber.
- Step 11** Under Message Waiting Indicators (MWIs), check the **Use MWI for Message Notification** check box.
- Step 12** In the Extension field, enter **x**.
- Step 13** Click the **Save** icon.

Setting Up for a Single-Line Test (Circuit-Switched Phone System Integrations Only)

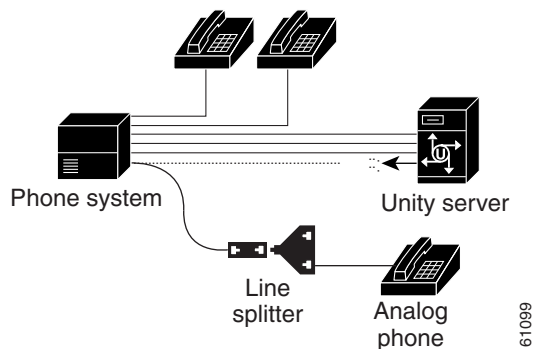
To do diagnostic tests, you need a lineman test set or an analog phone with a ringer. Additional equipment and the method you use to set up for a single-line test depend on the type of voice cards in the Cisco Unity server.

Because single lines cannot be split out from T1 digital cables, it is not possible to set up single-line testing for integrations that use T1 cables.

To Set Up a Dialogic D/120 Card for Single-Line Testing

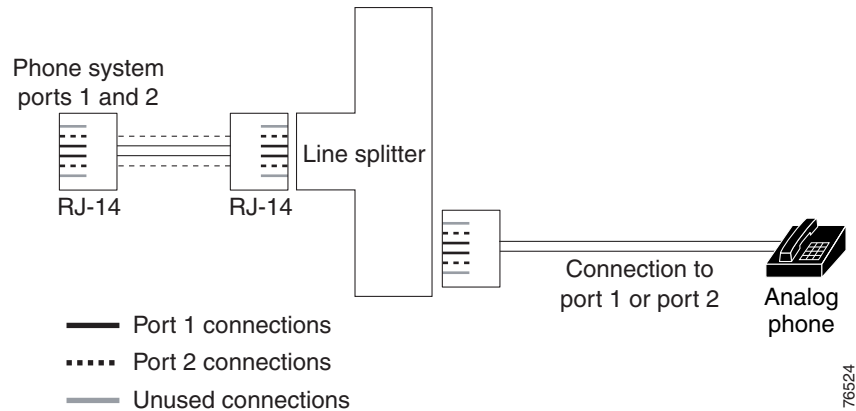
This voice card supports two lines per jack, so you need a line splitter to test individual lines.

- Step 1** Determine which line you are having trouble with, and unplug it from the voice card.



- Step 2** Plug that line into a line splitter.

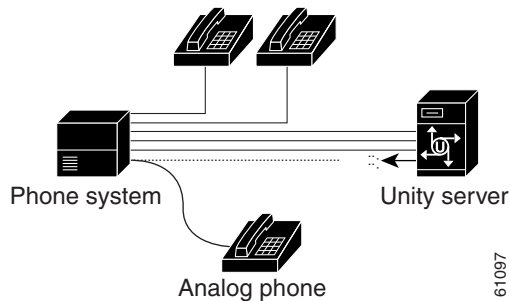
- Step 3** Plug the test phone into the jack on the line splitter corresponding to the port that you are having trouble with. The middle pair of wires (numbers 3 and 4) correspond to the first port, and the next pair of wires (numbers 2 and 5) correspond to the second port. The outer pair of wires (numbers 1 and 6) are unused.



To Set Up a Dialogic D/41 Card for Single-Line Testing

This voice card supports only one line per jack.

- Step 1** Determine which line you are having trouble with, and unplug it from the voice card.



- Step 2** Plug that line into the test phone.

Reporting Problems to Cisco TAC

When you report a problem to the Cisco Technical Assistance Center (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. Some of this information can be obtained by using the Gather Unity System Info utility, available in Tools Depot.

- Cisco Unity version currently in use. See one of the following procedures: [To Determine the Cisco Unity Version in Use by Using the Cisco Unity Administrator, page 1-4](#), or [To Determine the Cisco Unity Version in Use by Using the AvCsMgr.exe File, page 1-4](#).
- Cisco Unity-CM TSP version currently in use. See the procedure [To Determine the Cisco Unity-CM TSP Version in Use by Using the Avskinny.tsp File, page 1-5](#).



Note In versions earlier than 3.1(1), the Cisco Unity-CM TSP was known as the AV-Cisco TSP.

- RealSpeak TTS version currently in use. See the procedure [To Determine the RealSpeak ENU Language Engine in Use, page 1-5](#).
- Build number(s) of any software releases or upgrades installed.
- Number, type, and speed of processors.
- Memory and pagefile size.
- Hard disk size and free space available.
- Number and type of voice ports installed.
- Phone system integration, including the manufacturer, model, and version (if applicable).
- Cisco Unity switch.ini file version currently in use. See the procedure [To Determine the Switch.ini File Version in Use, page 1-5](#).
- Other telephony software or hardware installed, such as fax or UniModem.
- Microsoft Windows 2000 service packs installed.
- Number of subscribers in the Cisco Unity database.
- Approximate normal Cisco Unity 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 Determine the Cisco Unity Version in Use by Using the Cisco Unity Administrator

-
- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Software Versions** page. The version is displayed in the Cisco Unity Version field.
-

To Determine the Cisco Unity Version in Use by Using the AvCsMgr.exe File

-
- Step 1** Browse to the CommServer directory.
- Step 2** Right-click **AvCsMgr.exe**, and click **Properties**.
- Step 3** In the Properties window, click the **Version** tab.
- Step 4** In the Item Name list, click **Product Version**. The Cisco Unity version is displayed in the Value window.
-

To Determine the Cisco Unity-CM TSP Version in Use by Using the Cisco Unity Telephony Integration Manager

- Step 1** In the Cisco Unity Telephony Integration Manager, go to the **Cisco CallManager > Properties** page. The Cisco Unity-CM TSP version is displayed in the TSP Version field.
-

To Determine the Cisco Unity-CM TSP Version in Use by Using the Avskinny.tsp File

- Step 1** Browse to the WinNT\System32 directory.
- Step 2** Right-click the **Avskinny.tsp** file, and select **Properties**.
- Step 3** In the Properties window, click the **Version** tab.
- Step 4** The File Version value is the Cisco Unity-CM TSP version currently in use.
-

To Determine the Switch.ini File Version in Use

- Step 1** Browse to the CommServer directory.
- Step 2** Double-click **Editswitch.exe**.
- Step 3** Click **Edit This Switch Configuration**.
- Step 4** The Switch.ini file version is displayed in the title bar of the window.
-

To Determine the RealSpeak ENU Language Engine in Use

- Step 1** Browse to the CommServer\RealSpeak\Engine directory.
- Step 2** Right-click the file **Enu_g2p.dll**, and click **Properties**.
- Step 3** Click the **Version** tab.
- Step 4** The File Version value shown is the DLL version. The DLL versions correspond to the following RealSpeak versions:
- 3.6.0.0 = RealSpeak ENU language engine version 3.0(1)
 - 2.11.0.0 = RealSpeak ENU language engine version 2.1(1)
 - 2.1.0.0 = RealSpeak ENU language engine version 2.0(1)
-

To Determine the RealSpeak Base Engine Version in Use

- Step 1** Browse to the CommServer\RealSpeak\Api\Lib directory.
- Step 2** Right-click the file **Lhstts.dll**, and click **Properties**.
- Step 3** Click the **Version** tab.
- Step 4** The File Version shown is the DLL version. The DLL versions correspond to the following RealSpeak versions:
-

- 2.13.0.0 = RealSpeak base engine version 3.0(1)
 - 2.12.0.0 = RealSpeak base engine version 3.0(0)
 - 2.11.0.0 = RealSpeak base engine version 2.1(1)
 - 2.1.0.0 = RealSpeak base engine version 2.0(1)
-

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 subscriber 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 (see the “[Logs and Traces](#)” chapter for more information on how to obtain log and trace files).



Logs and Traces

In this chapter you will find information to help you gather logs and traces when troubleshooting Cisco Unity.

Cisco Unity and Third-Party Logs and Traces

For problems in the Miu or TSP, Cisco TAC may ask for logs and traces before the problem can be diagnosed and fixed. Miu diagnostic logs, along with the Event log and/or Dr. Watson logs, if available, are usually sufficient for the initial phase of diagnosing a problem.



Caution

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

See the following sections for details about third-party logs and traces:

- [Dr. Watson Logs, page 2-1](#)
- [Event Log Traces, page 2-2](#)

Most Cisco Unity components such as the Miu, Arbiter, Notifier, Conversations, and the Cisco Unity Administrator (also known as the “SA” or “System Administrator”) can write diagnostic information to a log file. Diagnostic output of the problem occurring is critical to determining what caused the problem. If the problem seldom occurs, such as only once a day, it can be difficult to find the actual occurrence of the problem in the diagnostic log.

See the following sections for details about Cisco Unity diagnostic traces:

- [Miu Diagnostics, page 2-2](#)
- [TSP Traces, page 2-4](#)

Dr. Watson Logs

Dr. Watson is a program invoked by Windows 2000 when a serious problem occurs that is not handled by Cisco Unity. When Dr. Watson is invoked, a dialog box that contains an error message appears (for example, “Dr. Watson encountering an error in the AvCsMgr.exe process”). Dr. Watson errors may occur in other processes such as Tapisrv.exe and Dlgc_srv.exe.

To Obtain a Dr. Watson Log

- Step 1** When a Dr. Watson error occurs, make a copy of the file **Winnt\Drwtsn32.log**.
 - Step 2** Before you attempt to reproduce the problem, from a command prompt, enter **drwtsn32** and press **Enter**.
 - Step 3** In the **Number of Instructions** field, enter **50**.
 - Step 4** In the **Number of Errors to Save** field, enter the number of errors you want to record. The default is 10.
 - Step 5** 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 6** Click **OK** to close the dialog box.
 - Step 7** Reproduce the problem.
 - Step 8** Make a copy of the file **Winnt\Drwtsn32.log**.
-

Event Log Traces

The Event log is used by Windows applications to report errors and warnings. The Miu reports serious failures to the Event log (for example, “Component Miu: thread <XXX> had a failure on port <YYY> in AvWav”).

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 Log**.
 - Step 3** Look for failure messages in the Application log. These can include errors from the Miu or AvWav, as well as errors from other Cisco Unity components.
 - Step 4** If failure messages are present in the Application log, in the Tree pane, click **Application Log**. Then, on the Action menu, click **Save Log File As**.
 - Step 5** In the Save as Type field, click **CSV**, then click **Save**. Do not save the raw Event log data in a *.evt file.
-

Miu Diagnostics

Enable the Miu diagnostics when you are obtaining traces for an Miu problem. For example, if there are AvWav errors in the Event log, enable the AvWav diagnostics. However, keep in mind that running additional diagnostics can affect system performance and hard drive space.

You can use micro traces to set individual levels for selected MUI traces, or you can use macro traces to select preset combinations of traces.

To Obtain Micro Trace Miu Diagnostics

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

- Step 2** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon. 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 for selected traces in components beginning with **Miu**.
- Step 5** Click **Next**.
- Step 6** On the Completing page, click **Finish**.
- Step 7** On the Cisco Unity Diagnostic Viewer screen, click the **Start New Log Files** icon.
- Step 8** Reproduce the problem.
- Step 9** To view the log files, in the Tree pane, click **Processes > AvCsMgr**, and then click the **Current** log file.
- Step 10** The selected log file appears in the right pane.
- Step 11** To export or save a copy of the log file, on the Action menu, click **Export List**.
- Step 12** Name the file and save it to a location of your choice in .txt or .csv format, then click **Save**.
- Step 13** To turn off the traces set in [Step 4](#), on the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 14** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.
-

To Obtain Macro Trace Miu Diagnostics

- Step 1** On the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.
- Step 2** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Macro Traces** icon. 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 selected traces.
- Step 5** Click **Next**.
- Step 6** On the Completing page, click **Finish**.
- Step 7** On the Cisco Unity Diagnostic Viewer screen, click the **Start New Log Files** icon.
- Step 8** Reproduce the problem.
- Step 9** To view the log files, in the Tree pane, click **Processes > AvCsMgr**, and then click the **Current** log file.
- Step 10** The selected log file appears in the right pane.
- Step 11** To export or save a copy of the log file, on the Action menu, click **Export List**.
- Step 12** Name the file and save it to a location of your choice in .txt or .csv format, then click **Save**.
- Step 13** To turn off the traces set in [Step 4](#), on the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 14** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.
-

TSP Traces

If Cisco TAC determines that TSP traces are needed, they will ask you to provide them.

To Obtain Cisco Unity-CM TSP Traces

- Step 1** Confirm that the clocks on Cisco Unity and Cisco CallManager are synchronized.
- Step 2** Enable tracing on the Cisco CallManager system.
- Step 3** On the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

- Step 4** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Macro Traces** icon. The Configure Macro Traces wizard appears.
- Step 5** On the Welcome page, click **Next**.
- Step 6** On the Configure Macro Traces page, check the **Skinny TSP** check box.
- Step 7** Click **Next**.
- Step 8** On the Completing page, click **Finish**.
- Step 9** On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.
- Step 10** Reproduce the problem.
- Step 11** To view the log files, in the Tree pane, click **Processes > Svchost**, and then click the **Current** log file.
- Step 12** The selected log file is appears in the right pane.
- Step 13** To export or save a copy of the log file, on the Action menu, click **Export List**.
- Step 14** Name the file and save it to a location of your choice in .txt or .csv format, then click **Save**.
- Step 15** To turn off the traces set in [Step 6](#), on the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 16** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.

Domino Directory Monitor Diagnostic Traces

You use the Unity Diagnostic Tool to set micro traces for the Domino directory monitor. The micro traces to enable are in the DSDomino group.

Flags to Enable

- If the creation, modification, or deletion of subscriber accounts, distribution lists, or location objects in the Cisco Unity Administrator fails, enable flags, 00, 11, 12, and 17.
- If changes made in the Domino directory are not reflected in Cisco Unity, enable flags 15, 16, and 17.
- If the directory monitor service logs an error to the Windows Event log saying that it has thrown an exception, enable flags 00, 01, and 18.

See [Table 2-1](#) for descriptions of the diagnostic flags.

Table 2-1 Diagnostic Flags for the Domino Directory Monitor

Diagnostic Flag	Description
00—High Level, Method Entry and Exit, and Parameter Values	Traces Cisco Unity Administrator calls to create, modify, delete, and find subscribers, distribution lists, and locations. Also traces calls to get and set system configuration parameters.
01—Low Level, Method Entry and Exit, and Parameter Values	Traces internal methods calls. Note that enabling this flag will produce very large diagnostic files.
02—Memory	Traces memory allocation and deallocation. There is seldom a need to enable this flag.

Table 2-1 Diagnostic Flags for the Domino Directory Monitor (continued)

Diagnostic Flag	Description
10—Password Crypt	Traces handling of the Notes User ID and password.
11—CallProgress	Traces milestones in the internal methods used for importing, updating, and deleting subscribers, distribution lists, and location objects.
12—Method Parameters	Traces the parameters in the internal methods used for importing, updating, and deleting subscribers, distribution lists, and location objects.
13—Sync Start End	Traces synchronization initialization.
14—Monitor Initialization	Traces the initialization of the directory monitor service.
15—DB Access	Traces access to the SQL database on the Cisco Unity server.
16—Sync Progress	Traces milestones during synchronization. Synchronization happens every minute.
17—Errors	Traces internal API errors.
18—Notes API Errors	Traces errors from the Notes API.
19—Notes Fields Read and Write	Traces Notes reads and writes. Note that enabling this flag will produce very large diagnostic files.



Internal and External Calls

About Problems with Internal and External Calls

Call problems fall into two categories:

No internal or external calls are answered	Problems that prevent internal calls from being answered are a subset of problems that prevent external calls from being answered. See the “Cisco Unity Is Not Answering Any Internal and/or External Calls” section on page 3-1.
Some internal or external calls are answered	If you determine that the problem occurs only with some internal or external calls, see the “Cisco Unity Is Not Answering Some Internal or External Calls” section on page 3-5.

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

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

There are several possible reasons that Cisco Unity may not answer any internal and/or external calls. Use the [“Task List for Troubleshooting No Answers on Incoming Calls”](#) to troubleshoot the possible causes.

Task List for Troubleshooting No Answers on Incoming Calls

1. Confirm that the phone system settings are correct. See the [“Confirming the Phone System Settings”](#) section on page 3-2.
2. (Serial integrations only) Confirm that a COM port is available. See the [“Confirming That a COM Port Is Available to Cisco Unity \(Serial or SMDI Integrations Only\)”](#) section on page 3-2.
3. If callers hear a reorder tone or dead air shortly after Cisco Unity startup, enable the ForceGlobalAcmThreadSafety Registry Setting. See the [“Enabling the ForceGlobalAcmThreadSafety Registry Setting When Corruption in Windows ACM Causes Callers to Hear Reorder Tone or Dead Air Shortly After Cisco Unity Startup”](#) section on page 3-3.
4. (Circuit-switched systems only) Confirm that the phone system generates a ring signal. See the [“Confirming That the Phone System Generates a Ring Signal \(Circuit-Switched Systems Only\)”](#) section on page 3-5.

Confirming the Phone System Settings

When the phone system settings in the Cisco Unity Telephony Integration Manager (UTIM) do not match the type of phone system that Cisco Unity is connected to, Cisco Unity may not answer calls.

To Confirm the Phone System Settings in UTIM

-
- Step 1** On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. UTIM appears.
 - Step 2** Confirm that the settings match those indicated in the integration guide for your phone system.
 - Step 3** Correct any incorrect values for the phone system.
 - Step 4** If you changed values in [Step 3](#), click **Save**.
 - Step 5** If prompted, restart the Cisco Unity server.
-

Confirming That a COM Port Is Available to Cisco Unity (Serial or SMDI Integrations Only)

Serial or SMDI traffic during a Windows startup may result in Windows assigning the COM port to a serial mouse, thus making the COM port unavailable to Cisco Unity. When Windows starts, it searches for the pointing device (usually a mouse). If a serial mouse is detected, Windows disables the port so that a device driver for the mouse can load instead. If no device is detected, Windows disables the port. A disabled COM port does not display any information in Control Panel > Ports.

If the serial integration was working correctly before shutting down and restarting the Cisco Unity server, but not after, do the following procedure to determine whether the COM port is available.

To View COM Port Assignments

-
- Step 1** On the Windows Start menu, click **Control Panel > Ports**.
 - Step 2** Look to see if the COM port connected to the serial cable, usually COM1, is listed in the Ports box.
If the COM port for the serial integration is listed, skip to the [“Confirming That the Phone System Generates a Ring Signal \(Circuit-Switched Systems Only\)”](#) section on page 3-5.
If the COM port for the serial integration is not listed, continue with [Step 3](#).
 - Step 3** On the Windows Start menu, click **Run**. Enter **Regedit** and click **OK**.
 - Step 4** Expand the key HKEY_LOCAL_MACHINE\Hardware\Description\System\MultifunctionAdapter.
 - Step 5** Click folder **4**, **5**, or **6** and locate the SerialController folder.
 - Step 6** The SerialController folder contains folders with a single-digit numeric designation (0, 1, and so on). Click the folder that corresponds to the serial integration COM port number.
 - Step 7** Double-click the **Identifier** key in the folder you chose in [Step 6](#). If the Identifier key Value Data refers to a mouse—for example Microsoft Ballpoint Serial Mouse—instead of a COM port (COM1, COM2, and so on), continue with the [“To Disable the Detection of Devices on COM Ports in Windows”](#) procedure.
-

To Disable the Detection of Devices on COM Ports in Windows

- Step 1** Make a backup copy of the **Boot.ini** file.
- Step 2** Remove the Hidden, System, and Read-only attributes from the **Boot.ini** file.
- Step 3** Open the **Boot.ini** file by using a text editor such as Notepad.
- Step 4** Add the **/NoSerialMice** option to the end of each entry in the [operating systems] section of Boot.ini. The **/NoSerialMice** option is not case sensitive. See the following list for syntax options.

/NoSerialMice	Disables the detection of serial mice on all COM ports.
/NoSerialMice:COM<x>	Disables the detection of serial mice on the COM<x> port.
/NoSerialMice:COM<x,y,z>	Disables the detection of serial mice on COM<x, y and z> ports.

Sample Windows Boot.ini file with **/NoSerialMice** option added:

```
[boot loader]
timeout=3
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT35
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT35="Windows NT Workstation
Version 3.51" /NoSerialMice
multi(0)disk(0)rdisk(0)partition(1)\WINNT35="Windows NT Workstation
Version 3.51 [VGA mode]" /basevideo /sos /NoSerialMice
```

- Step 5** Save the **Boot.ini** file, and exit the text editor.
- Step 6** Restore the Hidden, System, and Read-only attributes to the **Boot.ini** file.
- Step 7** Shut down and restart Windows.

Enabling the ForceGlobalAcmThreadSafety Registry Setting When Corruption in Windows ACM Causes Callers to Hear Reorder Tone or Dead Air Shortly After Cisco Unity Startup

A few sites have experienced a problem when using both G.711 and G.729a codecs with Cisco Unity. The problem occurs shortly after Cisco Unity starts. Calls received immediately after startup are answered, but within a few minutes, Cisco Unity stops answering calls.

This problem occurs only when all of the following conditions are present:

- When transcoding between G.729a and G.711 codecs is required in a Cisco Unity system. This includes any instances of G.729a prompts, messages, or greetings, even if Cisco Unity is in a G.711 region. The possibility that this problem can exist on a G.711 system has not been completely ruled out.
- When there are identical sequences of Miu wave errors in the Event log from more than one port at the same time, beginning with:

Component Miu: Thread 0x<NUM> had a Failure on Port X in AvWav

There will usually be four to six of these errors from one port intermingled with an identical sequence of four to six errors from another port. Errors from other ports may also be present.

- When the problem occurs within a few minutes of system startup, and when it can be consistently reproduced. When this happens, restarting the Cisco Unity server eliminates the problem temporarily, but it reoccurs. If a problem with similar symptoms occurs days after startup, or is sporadic, it is likely a different problem.

When Cisco Unity transcodes wave formats, it uses Microsoft Windows Audio Compression Manager (ACM) to call into the third-party G.729a codec. When multiple threads call into the Windows ACM function `AcmStreamConvert()` at the same time, they can conflict with one another and generate errors, causing callers to hear dead air or the reorder tone. Restarting the Cisco Unity server clears the corruption in Windows ACM temporarily, but it does not prevent the problem from reoccurring.

An application-level workaround, an optional registry setting, makes Windows ACM globally thread-safe. To enable the registry setting, do the following procedure.

To Enable the ForceGlobalAcmThreadSafety Registry Setting

This procedure is not required on all systems that use transcoding. Because it can have a performance impact, it should be done only if all of the conditions listed above are present.

Step 1 Start Regedit.



Caution

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

- Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
- Step 3** Expand the key `HKEY_LOCAL_MACHINE\Software\ActiveVoice`.
- Step 4** On the Edit menu, click **New Key**.
- Step 5** Name the new key **UnityAvWav**.
- Step 6** Click the new **UnityAvWav** key, then on the Edit menu, click **New Key**.
- Step 7** Name the new key **1.0**.
- Step 8** Click the new **1.0** key, then on the Edit menu, click **New Dword**.
- Step 9** Name the new Dword **ForceGlobalAcmThreadSafety**, and set the Value to **1**.
- Step 10** Close the Registry Editor.
- Step 11** Restart the Cisco Unity server for the settings to take effect.
- Step 12** Confirm that the problem does not reoccur within the first few minutes after Cisco Unity restarts. If the problem does reoccur, set the ForceGlobalAcmThreadSafety DWORD Value back to **0**, to avoid a system performance impact. Contact Cisco TAC for further assistance.
-

Confirming That the Phone System Generates a Ring Signal (Circuit-Switched Systems Only)

In order for Cisco Unity to answer calls, all ports and trunks must be configured correctly.

To Test Whether the Phone System Is Generating a Ring Signal

-
- Step 1** Set up a test phone (Phone 1) for single-line testing. For more information, see the [“Preparations for Troubleshooting the Phone System”](#) section on page 1-1.
- Step 2** On an extension that is connected to the phone system but that is not connected to Cisco Unity (Phone 2), call Phone 1.
- If Phone 1 rings, the phone system recognizes the port and is generating a ring signal.
- If Phone 1 does not ring, skip to [Step 6](#).
- Step 3** Repeat [Step 2](#) for each extension that is normally connected to Cisco Unity.
- Step 4** On Phone 2, dial the access code necessary to get an external line, then call Phone 1.
- If Phone 1 rings, the trunk is configured correctly to be answered by Cisco Unity ports. Continue with [Step 5](#).
- If Phone 1 does not ring, skip to [Step 6](#).
- Step 5** Repeat [Step 4](#) for each extension that is normally connected to Cisco Unity.
- Step 6** Verify the phone system programming, and change values as necessary.
- Step 7** Confirm that the wiring and the jacks are securely connected.
- Step 8** Repeat [Step 1](#) through [Step 5](#).
- If Phone 1 rings for each extension tested, the phone system is generating a ring signal and the ports and trunks are programmed correctly.
- If Phone 1 still does not ring for each extension tested, contact the phone system vendor.
-

Cisco Unity Is Not Answering Some Internal or External Calls

There are several possible reasons that Cisco Unity 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 hunt group programming is correct. See the [“Confirming Hunt Groups”](#) section on page 3-6.
2. Confirm that the routing rules are working correctly. See the [“Confirming Routing Rules”](#) section on page 3-7.
3. Verify that the number of licensed voice messaging ports is correct. See the [“Confirming Voice Messaging Port Licensing”](#) section on page 3-8.
4. 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 3-8.

5. Confirm that the phone lines and voice cards are working correctly. See the [“Confirming Phone Lines and Voice Cards”](#) section on page 3-9.

Confirming Hunt Groups

Depending on your phone system, do one of the following procedures, as applicable, to verify the hunt group programming for voice messaging ports on the phone system.

To Verify Hunt Group Programming for Voice Messaging Ports (Cisco CallManager Integration,)

-
- Step 1** In Cisco CallManager Administration, click **Service > Service Parameters**.
 - Step 2** On the Service Parameters Configuration page, click the server on which Cisco CallManager is installed.
 - Step 3** In the Configured Services list, click **Cisco CallManager**.
 - Step 4** In the Configured Service Parameters list, click **VoiceMailMaximumHopCount**.
 - Step 5** Confirm that VoiceMailMaximumHopCount is set to a value of two times the number of Cisco CallManager ports connected to Cisco Unity.
For example, on a 48-port system, the VoiceMailMaximumHopCount should be set to 50.
 - Step 6** Confirm that the voice messaging ports are set to forward both when busy and when not answered.
 - Step 7** Set up two test phones. For more information, see the [“Setting Up For a Diagnostic Test \(Cisco CallManager or SIP Integrations Only\)”](#) section on page 1-1.
 - Step 8** From a phone (not either of the test phones), dial the extension of the first voice messaging port, and leave the voice messaging port in a busy state.
 - Step 9** Access an external line from test Phone 2, and call test Phone 1. The first available port should take the call.
 - Step 10** Release the busy voice messaging port.
 - Step 11** In the Cisco Unity Administrator, go to the **System > Ports** page, and disable the port you just tested by unchecking the **Enabled** check box for that port.
 - Step 12** From a phone (not either of the test phones), dial the extension of the next voice messaging port, and leave the voice messaging port in a busy state.
 - Step 13** Repeat [Step 9](#) through [Step 12](#) until all the voice messaging ports have been tested in a busy state. When all voice messaging ports are disabled, and the last port is busy, Cisco CallManager should do whatever you programmed it to do when all lines are busy, such as forward the call to the attendant number. If this does not happen, change the Cisco CallManager programming and repeat the test.
-

To Verify Hunt Group Programming (Circuit-Switched Phone Systems Only)

-
- Step 1** Set up a test phone (Phone 1) for single-line testing. For more information, see the [“Preparations for Troubleshooting the Phone System”](#) section on page 1-1.
 - Step 2** Connect Phone 1 to the last line in the first hunt group.
 - Step 3** Busy every extension in the first hunt group except the last one by using the phone system programming.
 - Step 4** From an extension that is connected to the phone system but that is not connected to Cisco Unity (Phone 2), dial the first hunt group pilot number.

If Phone 1 rings, continue with [Step 5](#).

If you hear the busy tone or if Phone 1 does not ring, verify the phone system programming for the first hunt group and change values as necessary, and repeat this step. If Phone 1 still does not ring, contact the phone system vendor.

Step 5 Busy the last extension, so that every extension in the first hunt group is busied.

Step 6 On Phone 2, dial the first hunt group pilot number again.

If you hear the busy tone, the first hunt group is programmed correctly.

If you do not hear the busy tone, verify the phone system programming for the first hunt group and change values as necessary, and repeat this step. If you still do not hear the busy tone, contact the phone system vendor.

For details on programming hunt groups, see the documentation for your phone system.

Step 7 Repeat [Step 1](#) through [Step 6](#) for each hunt group.

Confirming Routing Rules

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

To Confirm That Cisco Unity Routing Rules Are Working Correctly

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

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

Step 3 On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon.

Step 4 In the Groups list, click **Arbiter**.

Step 5 In the Flags list, click **Diagnostics 14, 15, and 16**.

Step 6 In the Groups list, click **Ruler Domain**.

Step 7 In the Flags list, click **Diagnostic 11**.

Step 8 On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.

Step 9 Reproduce the problem.

Step 10 To view the log files, in the left pane of the Cisco Unity Diagnostic Viewer screen, click **Process > AvCsMgr**, and then click the **Current** log file.

Step 11 The selected log file is formatted and displayed in the right pane.

Step 12 To export or save a copy of the log file, click **Action > Export List**.

Step 13 Name the file and save it to a location of your choice in .txt or .csv format.

Step 14 To turn off the traces set in [Step 4](#) through [Step 7](#), on the Cisco Unity Diagnostic Viewer screen, click **Disable All Traces**.

Step 15 Browse to the `\CommServer\TechTools` directory.

Step 16 Open the `AvRulerEditor`.

Step 17 Click **Routing** to view the actual conditions of routing rules. 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 18** If you need to make a change to a routing rule, in the Cisco Unity Administrator, go to the **Call Management > Call Routing** page.



Note Do not use AvRulerEditor to change routing rules.

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 or AvRulerEditor, contact Cisco TAC.

Confirming Voice Messaging Port Licensing

When more voice messaging ports are installed on the Cisco Unity server than are licensed, Cisco Unity does not answer calls on the extra ports. (For example, if the voice cards in the Cisco Unity server have 48 ports but only 24 ports are licensed, Cisco Unity will answer calls only on the first 24 ports.)

To Confirm the Number of Ports

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Licensing**.
- Step 2** Confirm that the Voice Ports value matches the number of ports on the voice cards.
- If the values match, continue with the following [“Confirming Voice Messaging Port Settings”](#) section. If the value is smaller than the number of ports on voice cards in the Cisco Unity server, contact your sales representative.

Confirming Voice Messaging Port Settings

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

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

- Step 1** In the Cisco Unity Administrator, go to the **System > Ports** page.
- Step 2** Note which ports are designated to answer calls.
- Step 3** In the phone system programming, confirm that calls are being sent only to those ports designated to answer calls. Change the phone system programming if necessary.
- Step 4** If you made a change to the phone system programming in [Step 3](#), shut down and restart the Cisco Unity server to clear any hung ports.

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

To Confirm That Voice Messaging Ports Are Set Correctly

- Step 1** In the Cisco Unity Administrator, go to the **System > Ports** page.

- Step 2** Verify the settings for each voice messaging port, as follows:
- If a port is not enabled, check the **Enabled** check box to enable it.
 - If all of the ports are enabled and set correctly, continue with the [“Confirming Phone Lines and Voice Cards”](#) section on page 3-9.
 - If all of the ports cannot be enabled by using the Cisco Unity Administrator, do the following [“To Enable Voice Messaging Ports in the Registry”](#) procedure.
-

To Enable Voice Messaging Ports in the Registry



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

- Step 1** On the Windows Start menu, click **Run**.
- Step 2** Enter **Regedit** and click **OK**.
- Step 3** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
- Step 4** Expand the key
HKEY_LOCAL_MACHINE\Software\ActiveVoice\Arbiter\1.0\PortConfiguration\Dev<n>
where <n> is the number of the disabled port.
- Step 5** Double-click **Capabilities**.
- Step 6** In the Edit Dword Value window, change the Capabilities to **0xffffffff**.
- Step 7** Expand the key
HKEY_LOCAL_MACHINE\Software\ActiveVoice\Miu\1.0\Initialization\Port<n>
where <n> is the number of the disabled port.
- Step 8** Change the OfflineStatus to **0x0**.
- Step 9** Restart the Cisco Unity server.
- Step 10** In the Cisco Unity Administrator, go to the **System > Ports** page.
Confirm that all ports are enabled. If a port is still not enabled, contact Cisco TAC.
-

Confirming Phone Lines and Voice Cards

To Isolate a Problem with a Phone Line or Voice Card

- Step 1** Swap the phone lines from one jack to another on a voice card.
If the problem follows a phone line, the problem is in the phone line.
- Step 2** Swap the phone lines from a jack on one voice card to a jack on another voice card.

If the problem follows a jack, the problem is in the jack.

Step 3 Swap the locations of voice cards.

If the problem follows a voice card, the problem is in the card.

For information on testing Dialogic voice cards, see the “[Universal Dialogic Diagnostics Utility](#)” section on page 12-14.



Call Transfers

About Call Transfer Problems

Call transfer problems fall into two categories:

Problems on a newly installed or upgraded system	For call transfer problems that occur on newly installed systems or on systems that have just been upgraded, refer to the Cisco Unity integration guide for your system.
Problems on an existing system	See the “Calls Are Not Transferred to the Correct Greeting” section on page 4-1, or the “Subscriber Hears a Reorder Tone When Answering a Call from Cisco Unity” section on page 4-3.

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. See the [“Confirming That the Forward Timer in the Phone System Is in Synchrony with the Rings to Wait For Setting in Cisco Unity”](#) section on page 4-2.
2. Confirm that the phone system programming enables callers to hear the subscriber personal greeting. See the [“Confirming That the Phone System Programming Enables Callers to Hear the Subscriber Personal Greeting”](#) section on page 4-3.

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

For supervised transfers, the number of rings that Cisco Unity waits before routing a call to a subscriber 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 Cisco Unity waits before taking a message.

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

- The caller does not hear the beginning of the subscriber personal greeting. (For example, the subscriber 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 subscriber personal greeting.
- 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 the value of the forward timer.
- Step 2** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Call Transfer** page.
- Step 3** Click **Find**, and find the subscriber whose calls are not being routed to the correct greeting.
- Step 4** In the Transfer Incoming Calls to Subscriber’s Phone section, confirm that the **Yes, Ring Subscriber’s Extension** check box is checked.
- Step 5** In the Transfer Type section, confirm that the **Supervise Transfer** check box is checked.
- Step 6** In the Rings To Wait For box, the value should be two rings fewer than the value of the forward timer of the phone system, which you found in [Step 1](#); this value is typically not greater than four, and is never greater than eight. This value specifies the number of rings that Cisco Unity waits before routing the call to the subscriber personal greeting.

If the values do not meet the parameters, either reprogram the phone system so it waits longer before forwarding unanswered calls, or change the value in the Rings To Wait For box so that Cisco Unity routes the call before the phone system forwards it.

- Step 7** To change the default Rings To Wait For value for future subscribers, go to the **Subscribers > Subscriber Template > Call Transfer** page.



Note If you change the value in a subscriber template, the value is not changed for existing subscriber accounts that are based on that template. Changing the template affects only the value for subscriber accounts that are created after the template is changed.

- Step 8** Determine whether the phone system changes the ringback cadence after a certain number of rings. If it does so, in the Cisco Unity Administrator, set the Rings To Wait For value to a number fewer than the number of rings at the initial cadence.
- Step 9** If you have determined that the phone system is waiting longer to forward a call than Cisco Unity is waiting to take a message, but Cisco Unity still is not routing calls to the correct greeting, run the Learn Tones utility. For more information, see the [“Learn Tones” section on page 12-5](#).

If you have run the Learn Tones utility, and Cisco Unity still is not routing calls to the correct greeting, contact Cisco TAC.

Confirming That the Phone System Programming Enables Callers to Hear the Subscriber Personal Greeting

When callers hear the opening greeting instead of a subscriber personal greeting, confirm that the integration is enabled and that the phone system settings are correct. If the settings are incorrect, call forward to personal greeting and easy message access will not be enabled. Do one of the following procedures, depending on your phone system integration.

To Verify the Phone System Settings for the Integration (All Integrations)

- Step 1** On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
 - Step 2** Confirm that the settings match those indicated in the integration guide for your phone system.
 - Step 3** Correct any incorrect values for the phone system, and click **Save**.
 - Step 4** If prompted, restart the Cisco Unity server.
 - Step 5** If you have confirmed that the phone system settings are correct, and callers still hear the opening greeting after dialing the subscriber extension, contact Cisco TAC.
-

To Verify the Phone System Programming (Ericsson MD-110 Integration Only)

- Step 1** On the phone system, confirm that the Prefix digits for forwarded calls and for easy message access are programmed correctly.
 - Step 2** Confirm that the called extension has Coverage On No Answer set to forward to the voice messaging system.
-

Subscriber Hears a Reorder Tone When Answering a Call from Cisco Unity

A possible cause for this problem is that the Rings to Wait For settings are incorrect.

Cisco Unity requires a minimum setting of three rings to wait to properly transfer a call or to make a message notification call. If the number of rings to wait is set to fewer than three, a subscriber may hear the reorder tone instead of the Cisco Unity conversation.

To Correct the Rings to Wait For Settings

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
- Step 2** In the Notification Options section for each device used, set the Wait For How Many Rings Before Hanging Up field to three or more rings.
- Step 3** Go to the **Subscribers > Subscriber Template > Message Notification** page.
- Step 4** In the Notification Options section for each device used, confirm that the Wait For How Many Rings Before Hanging Up field is set to three or more rings, thus ensuring that future subscriber accounts get the correct default value.

If the default setting in the subscriber template is incorrect, you will need to change the value in all subscriber accounts that are based on that template.

- Step 5** Go to the **Call Management > Call Handlers > Call Transfer** page.
- Step 6** View the Standard, Alternate, and Closed rules. In the Transfer Type section, if Supervise Transfer is selected for any of the rules, confirm that the Rings To Wait For field is set to three or more rings.
- If Rings To Wait For is set correctly, and the subscriber still hears a reorder tone when answering a call from Cisco Unity, contact Cisco TAC.
-



Messages

About Problems with Messages

Message problems fall into the following categories:

Messages appear to be delayed	Some subscriber errors or misconceptions can lead to the impression that Cisco Unity is delaying messages. See the “Messages Appear to Be Delayed” section on page 5-1.
Messages seem to disappear	Some Cisco Unity situations can affect message delivery. See the “Some Messages Seem to Disappear” section on page 5-2.
Messages are incomplete	A setup problem may cause callers to be cut off when they try to leave a message. See the “Cisco Unity Stops Recording Before a Caller Has Finished Leaving a Message” section on page 5-3.
Messages include dial tone or reorder tone	See the “Dial Tone or Reorder Tone Is Present at the End of a Message” section on page 5-5.

Begin your troubleshooting by gathering information about the message problem. By discussing the problem with the subscriber, you can determine whether a problem is due to a misunderstanding of how Cisco Unity works. If you encounter a message problem that is not described in this section, contact the Cisco Technical Assistance Center (TAC).

Messages Appear to Be Delayed

The following sections describe possible reasons that messages may appear to be delayed. Use the [“Task List for Troubleshooting Delay in Appearance of Messages”](#) to troubleshoot the possible causes.

Task List for Troubleshooting Delay in Appearance of Messages

1. Investigate whether the subscriber misunderstands how Cisco Unity delivers messages. See the [“Subscriber Misunderstandings”](#) section on page 5-2.
2. Check to see if the Domino server is down or disconnected. See the [“Cisco Unity Domino Server Is Down or Is Disconnected”](#) section on page 5-2.



Tip

To confirm the arrival times of messages, generate a subscriber message activity report for the subscriber. For more information, refer to the “Subscriber Message Activity Report” section in the “Reports” chapter of the *Cisco Unity System Administration Guide*. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.

Subscriber Misunderstandings

A Subscriber Who Is Using Optional Conversation 1 Misunderstands the Effect of Pressing the # Key Twice During Message Playback

When a subscriber presses the # key twice while listening to a message, Cisco Unity saves the message as a new message and skips to the next message. Later, the subscriber checks messages again, hears the same message, and believes the message arrived after a delay.

Explain to the subscriber that pressing the # key twice while a message plays saves it as a new message. Refer subscribers to the end-user documentation available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

A Subscriber Who Is Using the Standard Conversation Misunderstands the Effect of Pressing the # Key Twice During Message Playback

When a subscriber presses the # key twice while listening to a new message, Cisco Unity saves the message as a new message and skips to the next message. Later, the subscriber checks messages again, hears the same message, and believes the message arrived after a delay.

Explain to the subscriber that pressing the # key twice while a new message plays saves it as a new message. Refer subscribers to the end-user documentation available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

System Clock Time Is Incorrect

When the system clock is slow or when a desk clock is fast, the subscriber may believe messages were delayed.

Confirm that the system clock on the Cisco Unity server is reporting the correct time.

Cisco Unity Domino Server Is Down or Is Disconnected

Messages recorded while the Domino server (the message store) is down or disconnected are stored in the Unity Messaging Repository (UMR) until the server is brought back up. The delay experienced between the time a message is recorded and its delivery is entirely dependant on the amount of time that the message store was down or disconnected.

Some Messages Seem to Disappear

The following sections describe possible reasons that messages may not be delivered to the intended recipients. Use the “[Task List for Troubleshooting the Disappearance of Some Messages](#)” to troubleshoot the possible causes.

Task List for Troubleshooting the Disappearance of Some Messages

1. Verify that subscribers who are assigned to the Unaddressed Messages distribution list have been forwarding messages to the intended recipients. See the “[Undeliverable Messages Have Not Been Forwarded to Recipients](#)” section on page 5-3.
2. Confirm that you or another administrator did not inadvertently delete a subscriber who was assigned to review the messages for Cisco Unity entities. See the “[Subscribers Assigned to Cisco Unity Entities Were Deleted and No Replacements Were Assigned](#)” section on page 5-3.

Undeliverable Messages Have Not Been Forwarded to Recipients

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

Subscribers Assigned to Cisco Unity Entities Were Deleted and No Replacements Were Assigned

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

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

To identify call handlers that are associated with improperly deleted accounts, run the Unresolved References report. Then you can fix any “stranded” call handlers that you find by running the DbWalker utility. Refer to the “Reports” chapter of the *Cisco Unity System Administration Guide* for more information. The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.

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

The following sections describe possible reasons that Cisco Unity may stop recording before a caller has finished leaving a message. Use the “[Task List for Troubleshooting Recordings That Are Being Cut Off](#)” to troubleshoot the possible causes.


Task List for Troubleshooting Recordings That Are Being Cut Off

1. Check to see whether the quiet parameter is set to recognize low voice volume. See the “[Dialogic Quiet Parameter Is Incorrect](#)” section on page 5-4.
2. Calls may be cut off by Cisco Unity, the phone system, or the central office. See the “[Cisco Unity, the Phone System, or the Central Office Disconnected the Call](#)” section on page 5-4.

Dialogic Quiet Parameter Is Incorrect

A caller may report hearing a prompt and being prevented from completing a message, or a subscriber may report this problem after noticing that a recording ends before the caller finished leaving a message. This can happen when the quiet parameter is not set to recognize low voice volume. It can also happen when a changed quiet parameter is not retained after a Cisco Unity upgrade.

To Change the Dialogic Quiet Parameter (Systems Equipped with Dialogic Voice Cards Only)

-
- Step 1** Shut down the Cisco Unity software.
- Step 2** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
- Step 3** On the Service menu, click **Stop Service**. A second Dialogic Configuration Manager window appears.
- Step 4** When the message “Success: Dialogic service stopped” appears, click **Close**.
- Step 5** In the Service window, select a Dialogic voice card.
- Step 6** In the DCM–Properties dialog box for the card, click **Misc**.
- Step 7** Click **ParameterFile**.
- Step 8** Under Edit in the Value field, enter **quiet50.prm**, and click **OK**.
-  **Note** If spandti.prm or any other values exist in the Value field, enter a space at the end of the existing value, and enter **quiet50.prm**. The space ensures that both .prm entries exist in the field.
-
- Step 9** Repeat [Step 5](#) through [Step 8](#) for each additional Dialogic voice card.
- Step 10** On the Service menu, click **Start Service**. A second Dialogic Configuration Manager window appears.
- Step 11** When the message “Success: Dialogic service started” appears, click **Close**.
- Step 12** Restart the Cisco Unity server.
-

Cisco Unity, the Phone System, or the Central Office Disconnected the Call

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, 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** On the Log menu, click **System**.
- 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** On the Log menu, click **Application**.
- 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.
-

Dial Tone or Reorder Tone Is Present at the End of a Message

A possible cause may be that the switch disconnect tone and/or the PSTN disconnect tone are incorrect in the Switch.ini file (for circuit-switched phone systems only). Running the Learn Tones utility will correct the Switch.ini file so that Cisco Unity will recognize dial tone and reorder tone, preventing them from being recorded as part of a message.

To Run the Learn Tones Utility

-
- Step 1** Run the Learn Tones utility. See the [“Learn Tones” section on page 12-5](#) for detailed instructions.
- Step 2** If running the Learn Tones utility does not resolve the problem, contact Cisco TAC.
-

■ Dial Tone or Reorder Tone Is Present at the End of a Message



Audio Quality

About Audio Quality Problems

Audio quality problems can manifest themselves in a variety of ways, and can be difficult to diagnose and correct. For example, subscribers may report volume differences between messages and system prompts, or report that messages are distorted. Audio quality symptoms may not be present for every subscriber, or consistently appear on every message or every system prompt.

The entire device topology can affect audio quality, both within and outside of the control of Cisco Unity. Cisco Unity-controlled features include automatic gain control (AGC), the Cisco Unity-CM TSP wave gain, and the audio codec chosen for message storage. Cisco CallManager controls the region setting for the audio codec. Finally, the Cisco gateway gain and attenuation settings can also affect audio quality.

Audio Quality Problems in Cisco Unity

The most common symptom of audio quality problems in Cisco Unity is when the volume of greetings and voice names is higher or lower than the volume of Cisco Unity prompts.

See [Table 6-1](#) for basic corrective action to level all WAV files on the Cisco Unity server to the same value, and to adjust the playback level if needed.

Table 6-1 Basic Audio Quality Troubleshooting for Cisco Unity

Symptom	General Circumstances	Corrective Action
The volume of greetings and voice names is higher or lower than the volume of Cisco Unity prompts.	Only certain greetings and voice names may be affected, and/or An upgrade was performed recently.	<ol style="list-style-type: none"> 1. Confirm that the Cisco Unity-CM TSP wave gain playback and record settings are both set to 0. 2. Run the Set Volume Level utility to bring pre-upgrade greetings and voice names to the correct dB levels. 3. Check and adjust the Cisco Unity AGC settings, if necessary (set to -26 dB default value). 4. Check and adjust the Cisco Unity-CM TSP wave gain playback setting, if necessary. <p>For detailed instructions, see the “Set Volume Level Utility” section on page 6-2.</p>

Set Volume Level Utility

The Set Volume Level utility allows you to level all WAV files on the Cisco Unity server to the same value, and to adjust the playback level, if needed.

Because automatic gain control is enabled by default (in Cisco Unity version 3.1(2c) and later systems, and in Cisco CallManager and dual integration version 4.0(3) and later systems), after an upgrade you may experience a problem in which the existing greeting and name recordings sound louder than new greetings and names recorded after the upgrade.

The Cisco Unity registry setting AGCminimumThreshold controls the minimum dB level of an incoming recording that Cisco Unity attempts to adjust. The setting prevents both silence in a message and background hiss from being adjusted. The AGCminimumThreshold has a default setting of -45 dB and an allowable range of -35 dB to -55 dB.

To maximize success in resolving or avoiding volume problems, we recommend that you first upgrade to Cisco Unity version 4.0(3), then use the Set Volume utility to match the existing greeting and name recordings to the gain levels of Cisco Unity after the upgrade.


The following procedure levels all WAV files on the Cisco Unity server to the same value, and provides instructions for adjusting the playback level, if necessary.

To Adjust Greeting and Name Recordings by Using the Set Volume Utility

-
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** If you do not have a Cisco CallManager integration, skip to [Step 4](#).
If you have a Cisco CallManager integration, and the Cisco CallManager region is set to use the G.711 codec, in the left pane, under Administrative Tools, double-click **Wave Gain**.
- Step 3** Confirm that both Record Gain and Playback Gain are set to **0**.
- Step 4** In the left pane of the Tools Depot window, browse to Audio Management Tools, and double-click **Set Volume**.
- Step 5** In the Set Greetings and Voice Names window, click **Select All**.
- Step 6** Confirm that the Save Original Files check box is checked, then enter the location to which the backup copy of the original recorded names and greetings files will be saved.
- Step 7** In the Options section, verify that the values match those shown in the following table.

New Target dB	-26
Sample Size	8000
Max dB Adjustment	5
Min. dB Threshold	-45

- Step 8** Confirm that the Save Above Volume Options check box is checked. Note that setting New Target dB to a value other than zero turns on automatic gain control.
- Step 9** Click **Set Volume Level**.
- Step 10** When “Done” appears in the Set Volume window, all existing greeting and name recordings have been adjusted to the New Target dB level. Click **OK**, and then click **Exit**.

- Step 11** If you do not have a Cisco CallManager integration, you have completed all necessary steps in this procedure.
- If you have a Cisco CallManager integration, and the Cisco CallManager region is set to use the G.711 codec, start the Cisco Unity Administrator.
- Step 12** Go to any page in the Cisco Unity Administrator that contains a Media Master control bar, and verify that the phone is selected as the playback device.
-  **Note** In order to use the phone as a recording and playback device, Cisco Unity must have at least one port assigned for a TRAP Connection per session on the System > Ports page. Refer to the “Voice Messaging Port Settings” section in the “System Settings” chapter of the *Cisco Unity System Administration Guide* for more information. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.
- Step 13** Click **Play** on the Media Master control bar to listen to a recording (for example, a subscriber greeting) over the phone.
- If the volume of the recording is acceptable, you have completed all necessary steps in this procedure.
- If the volume of the recording is too quiet, continue with [Step 14](#).
- Step 14** In the left pane of the Tools Depot window, under Audio Management Tools, double-click **Wave Gain**.
- Step 15** Increase the **Playback Gain** value by one or two dB. Listen to the volume of a recording.
- If the volume of the recording is acceptable, note the Playback Gain value and continue with [Step 16](#).
- If the volume of the recording is still too quiet, repeat this step.
- Step 16** In the left pane of the Tools Depot window, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 17** In the Unity Settings pane, click **Set Wave Gain dB Adjustment for Playback**.
- Step 18** Enter the new value determined in [Step 15](#), and click **Set**.
- Step 19** When prompted, click **OK**. You do not need to restart the Cisco Unity server to enable the registry change.
- Step 20** Click **Exit**.

Advanced Audio Quality Troubleshooting in Cisco Unity

See [Table 6-2](#) for advanced corrective actions and links to other troubleshooting procedures and information for the following symptoms:

- Messages and/or Cisco Unity prompts sound distorted.
- A hissing sound is heard when there is no audio from Cisco Unity.
- Message playback volume is higher or lower than the volume of Cisco Unity prompts, in certain cases.
- TTY characters are garbled or missing.
- Callers can hear Cisco Unity prompts, but Cisco Unity does not transmit any audio when a caller speaks.

For additional advanced audio troubleshooting tools, see the “Audio Troubleshooting Utilities” section on page 6-11.

Table 6-2 Advanced Audio Quality Troubleshooting

Symptom	General Circumstances	Corrective Action
Messages and/or Cisco Unity prompts sound distorted.	You are using the G.729a codec for message storage and retrieval.	<ol style="list-style-type: none"> 1. Confirm that the G.729a codec is being used for message recording on Cisco Unity. See the “Set Record Format Utility” section on page 6-5. 2. Confirm that the Cisco CallManager region is set to G.729a. Refer to the applicable <i>Cisco CallManager Administration Guide</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_allmg/index.htm. 3. Confirm that the greetings and recorded names are in G.729a format. See the “To View Codec Information for Greetings, Voice Names, and System Prompts” section on page 6-5.
	You are using the G.711 codec for message storage and retrieval.	<ol style="list-style-type: none"> 1. Confirm that the Cisco CallManager region is set to G.711. Refer to the applicable <i>Cisco CallManager Administration Guide</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_allmg/index.htm. 2. Confirm that the greetings and recorded names are in G.711 format. See the “To View Codec Information for Greetings, Voice Names, and System Prompts” section on page 6-5.
	Outside caller messages only are affected.	Check the Cisco gateway gain and attenuation levels. Refer to the guide for your gateway, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/index.htm .
Hissing noise is heard when there is no audio from Cisco Unity, such as between system prompts or during transfers.	The problem can be reproduced on multiple subscriber phones.	Check the Cisco Unity comfort noise registry setting. See the procedure <i>To View and Adjust the Cisco Unity Comfort Noise Registry Setting</i> , page 6-10.
TTY characters are garbled or missing.	The problem occurs when using TTY phones.	Disable the Cisco Unity comfort noise registry setting. See the procedure <i>To View and Adjust the Cisco Unity Comfort Noise Registry Setting</i> , page 6-10.
Message playback volume is higher or lower than the volume of Cisco Unity prompts, in special cases.	Only outside caller messages are affected.	<ol style="list-style-type: none"> 1. Check the Cisco gateway gain and attenuation levels. Refer to the guide for your gateway, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/index.htm. 2. Check the Cisco Unity-CM TSP wave gain playback and record settings. See the “Cisco Unity-CM TSP Wave Gain” section on page 6-6.
	Both subscriber and outside caller messages are affected.	Check the Cisco Unity-CM TSP wave gain playback and record settings. See the “Cisco Unity-CM TSP Wave Gain” section on page 6-6.

Table 6-2 Advanced Audio Quality Troubleshooting (continued)

Symptom	General Circumstances	Corrective Action
Cisco Unity plays system prompts but does not transmit voice.	The Cisco Unity server has dual NICs.	See the “Cisco Unity Plays System Prompts but Does Not Transmit Voice” section on page 9-1.

Set Record Format Utility

The Set Record Format utility changes the recording codec used for all recordings on Cisco Unity. It is not possible to select user- or port-specific recording formats. Changes to the record format apply only to recordings made after the change takes place. The utility does not convert any existing messages or greetings to the new codec.

When the recording codec is changed on a Cisco Unity system that has been running for a while, it is possible that greetings, voice names, prompts, and messages may be stored in more than one format. Cisco Unity can transcode between formats; however, we do not recommend that you use mixed formats on very busy systems.

To view codec information for greetings, voice names, and prompts, do the procedure [To View Codec Information for Greetings, Voice Names, and System Prompts](#), page 6-5.

To change the codec used for all Cisco Unity recordings (messages, greetings, and voice names) do the procedure [To Change the Cisco Unity Recording Codec](#), page 6-5.

For information on choosing and implementing codecs, refer to the *White Paper: Audio Codecs and Cisco Unity*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpapr/codecs.htm.

To View Codec Information for Greetings, Voice Names, and System Prompts

-
- Step 1** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane of the Tools Depot window, under Audio Management Tools, double-click **Codec Checker**.
 - Step 3** To export the data to a CSV file, click **File**, then choose to export greeting and voice name data, or prompt data.
 - Step 4** Click **Exit**.
-

To Change the Cisco Unity Recording Codec

-
- Step 1** Exit the Cisco Unity software (right-click the Cisco Unity icon in the system tray, then click **Stop Cisco Unity**).
 - Step 2** To use the G.711 Mu-law or A-Law, G729a, or GSM 6.10 codec, skip to [Step 4](#).
 - Step 3** To use one of the optional Dialogic OKI ADPCM codecs:
 - a. Browse to the **Other Cisco Unity Components Software Download** page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity>.
 - b. Click **CiscoUnityDialogicCodec.exe**, and download the file to the directory of your choice on the Cisco Unity server.

- c. Unzip the **CiscoUnityDialogicCodec.exe** file to the directory of your choice.
 - d. Double-click **Avvox_setup.exe**, and follow the on-screen prompts.
- Step 4** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 5** In the left pane, under Audio Management Tools, double-click **Set Record Format**.
- Step 6** In the Format list, select a supported codec, and click **OK**.
- Step 7** Restart the Cisco Unity server.

To Change the Recording Format for Existing Greetings and Voice Names

- Step 1** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Audio Management Tools, double-click **Set Wav Format**.
- Step 3** Select the greetings and voice names to adjust.
- Step 4** Under Backup Original Voice Names and Greetings, check the check box, and enter the location to save the original files.
- Step 5** On the list, select the new WAV format.
- Step 6** Click **Set Wav Format**.
- Step 7** Click **OK**, then click **Exit**.
- Step 8** Restart the Cisco Unity server.

Cisco Unity-CM TSP Wave Gain

The registry keys shown in [Table 6-3](#) determine how the Cisco Unity-CM TSP adjusts record and playback volume for all recordings (messages, prompts, voice names, and greetings) for IP devices in a Cisco CallManager region that contains Cisco Unity and is set to use the G.711 codec.

These registry settings are only applicable with a Cisco CallManager integration. If you have a PBX integration that uses Dialogic voice cards, see the [“Dialogic Voice Card Automatic Gain Control and Registry Settings”](#) section on page 6-9.

Table 6-3 Cisco Unity-CM TSP Wave Gain Registry Settings

Key Name	Purpose	Recommended Setting
WaveDBGainPlayback	Controls the wave driver boost or the reduction of system-wide playback levels for all recordings.	0
WaveDBGainRecord	Controls the wave driver boost or the reduction of recordings system-wide.	0

Confirm that both the Cisco Unity-CM TSP Wave Gain record and playback levels are set to 0 by using the Wave Gain utility, available in the Audio Management section of Tools Depot.

If you have not already done so, do the procedure [To Adjust Greeting and Name Recordings by Using the Set Volume Utility](#), page 6-2.

Automatic Gain Control

Cisco Unity Automatic Gain Control and Registry Settings

Cisco Unity automatic gain control (AGC) gives subscribers consistent message playback levels through the normalization of recordings. AGC affects recordings only. It is on by default except for single legacy PBX integrations, is controlled by registry settings, and is applied to voice samples after they have passed through all external hardware.

AGC does not improve the quality of recordings; it only addresses volume issues. For example, it cannot improve garbled incoming messages.

Systems upgraded to version 4.0(3) from 3.1(2c) and earlier may experience a problem where the existing greeting and name recordings sound louder than new greetings and names recorded after the upgrade. To prevent or resolve this problem after an upgrade, use the Set Volume utility to match the existing greeting and name recordings to the gain levels of Cisco Unity after the upgrade. The default values for the registry settings should be used for all Cisco Unity upgrades. If you have not already done so, do the procedures in the [“Set Volume Level Utility”](#) section on page 6-2.

The registry keys shown in [Table 6-4](#) determine how Cisco Unity AGC normalizes recordings.

If you are using Dialogic voice cards with a single legacy PBX integration, Cisco Unity AGC is disabled by default for all upgrades and new version 4.0(3) and later installs. Cisco Unity AGC can be disabled manually in earlier versions if audio quality problems are encountered. See the procedure [To Disable Cisco Unity AGC \(for a Single Legacy PBX Integration Only\)](#), page 6-8.

If you are using Dialogic voice cards with a dual integration, we recommend that you disable Cisco Unity AGC on the ports assigned to the legacy PBX integration. See the procedure [To Disable Cisco Unity AGC \(for a Legacy PBX in a Dual Integration Only\)](#), page 6-8.

Table 6-4 Automatic Gain Control Registry Keys

Key Name	Purpose	Recommended Setting
AGCtargetDB	Target root mean square (RMS) power to which all recordings are normalized. The setting is system-wide.	–26 dB The accepted range is –18dB to –30dB A setting of 0 (zero) disables AGC
AGCsampleSize	Buffer sample size used to calculate the average RMS power level.	8000
AGCuseCompression	Determines if a sample is clipped when a gain adjustment is applied. A value of 1 will not clip the sample; 0 clips the sample to the minimum/maximum values.	1 (0 = clipped sample; disables compression)

Table 6-4 Automatic Gain Control Registry Keys (continued)

Key Name	Purpose	Recommended Setting
AGCgainThreshold	Maximum dB gain (+/-) applied to a sample to bring it to the target dB level.	5 dB
AGCminimumThreshold	Controls the minimum dB level of an incoming recording that Cisco Unity attempts to adjust. The setting prevents silence in a message and background hiss from being adjusted.	-45 dB The accepted range is -35 dB to -55 dB

To Disable Cisco Unity AGC (for a Single Legacy PBX Integration Only)

-
- Step 1** Exit the Cisco Unity Administrator.
 - Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 3** In the left pane of the Tools Depot window, browse to Audio Management Tools, and double-click **Set Volume**.
 - Step 4** In the Set Greetings and Voice Names window, click **Select All**.
 - Step 5** Confirm that the Save Original Files check box is checked, then enter the location to which the backup copy of the original recorded names and greetings files will be saved.
 - Step 6** In the Options section, set New Target dB to **0** (zero).
 - Step 7** Confirm that the Save Above Volume Options check box is checked. Note that setting New Target dB to a value other than zero turns on automatic gain control.
 - Step 8** Click **Set Volume Level**.
 - Step 9** When “Done” appears in the Set Volume window, all existing greeting and name recordings have been adjusted to the New Target dB level with AGC disabled.
 - Step 10** Click **OK**, and then click **Exit**.
-

To Disable Cisco Unity AGC (for a Legacy PBX in a Dual Integration Only)

-
- Step 1** On the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
 - Step 2** In the left pane, click **Integration > Properties** for the integration that is using Dialogic voice cards.
 - Step 3** Click the Gain Control tab.
 - Step 4** Uncheck the **Enable Automatic Gain Control for this Integration** check box.
 - Step 5** In the UTIM window, click **Save**.
-

Dialogic Voice Card Automatic Gain Control and Registry Settings

Dialogic voice cards adjust the volume of recorded messages by using their own on-board AGC. Adjusting the playback volume for all recordings on systems equipped with Dialogic voice cards is done by changing the Median Volume registry setting. This setting is also used in the case of a dual integration, when you want to change the output volume level on the PBX side without affecting the Cisco CallManager side.

If you are using Dialogic voice cards with a single switch integration, Cisco Unity AGC is disabled by default for all upgrades and new version 4.0(3) and later installs, and can be disabled manually in earlier versions if audio problems are encountered. See the procedure [To Disable Cisco Unity AGC \(for a Single Legacy PBX Integration Only\)](#), page 6-8.

If you are using Dialogic voice cards with a dual integration, we recommend that you disable Cisco Unity AGC on the ports assigned to the legacy PBX integration. See the procedure [To Disable Cisco Unity AGC \(for a Legacy PBX in a Dual Integration Only\)](#), page 6-8.

To Adjust the Playback Volume of Recordings for Cisco Unity Systems Equipped with Dialogic Voice Cards

Step 1 Start Regedit.



Caution

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

Step 2 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3 Using Regedit, expand the registry key

HKEY_LOCAL_MACHINE\Software\Active Voice\Miu\1.0\Initialization\Service Provider <n>\

where <n> is a single digit number. (There may be more than one Service Provider key on your system.) Locate the Service Provider key whose Service Provider Name is D41MT.TSP.

Step 4 Expand the MedianVolume key.

Step 5 In the Base window, click **Decimal**.

The default setting for analog voice cards is 50, and the accepted range is between 0 and 100. Note that this setting is not in decibels, and that the numerical values are not linear. For example, a setting of 100 is louder, but not twice as loud as 50. Make a small adjustment to this setting of no more than 10 units louder or quieter.

Step 6 To adjust the playback volume for Text to Speech recordings (TTS), browse to the Median TTS Volume key.

Step 7 In the Base window, click **Decimal**.

The default setting for analog voice cards is 50, and the accepted range is between 0 and 100. Like the Median Volume key, this setting is not in decibels, and the adjustments are not linear. Make a small adjustment to this setting of no more than 10 units louder or quieter.

Step 8 Restart the Cisco Unity server.

- Step 9** Test the playback levels of several recordings. If the volume levels are acceptable, you have completed all steps necessary in this procedure. If the volume levels are too high or too low, repeat [Step 3](#) through [Step 8](#), and retest until you are satisfied with the results.
-

Comfort Noise

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

Comfort noise is not sent over the network, and is audible only on the IP device that receives a comfort noise generation packet. Comfort noise generation packets are sent by Cisco Unity when it is integrated with Cisco CallManager, and when the registry setting `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Avaudio\Parameters\ComfortNoise` is enabled.

The Cisco Unity ComfortNoise registry setting is a system-wide setting that controls the ability of Cisco Unity to send comfort noise generation packets to an IP phone, or to a gateway that is enabled to receive and respond to comfort noise generation packets. This registry setting does not affect comfort noise generation on a call between two IP phones. Cisco Unity also does not respond to comfort noise generation packets sent by other devices. These packets are treated as silence at the wave driver level.

If subscribers hear an audible hissing noise when there is no audio from Cisco Unity, and if it is judged to be too loud a noise, confirm that the Cisco Unity comfort noise registry setting is enabled (set to a value other than 128), and adjust the setting to a lower value as needed. The default value set during the Cisco Unity-CM TSP install is -50dB .

If subscribers report that some Cisco Unity prompts sound mechanical or computerized when played back over the phone, this may be the result of a gateway-induced jitter buffer problem. Disabling Cisco Unity comfort noise resolves this issue.

If you are using the Cisco Unity TTY (ENX) language and TTY phones, and you are using direct connect mode to an FXS port (H.323 or MGCP to CCM3.3(2)), TTY subscribers may encounter occasional dropped or garbled TTY characters. Disabling the Cisco Unity comfort noise setting will correct this problem.

**Note**

The registry setting for Cisco Unity comfort noise does not reflect the minus sign, so a registry setting of “50” is actually -50dB .

There will always be some amount of hissing noise between prompts. The Cisco Unity ComfortNoise registry setting only tells the IP phone or gateway how loud that hiss should be. A value of 128 causes the IP phone or gateway to use its default hiss level.

To View and Adjust the Cisco Unity Comfort Noise Registry Setting

- Step 1** Start Regedit.

**Caution**

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

- Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.
- Step 3** Expand the registry key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Avaudio\Parameters\ComfortNoise.
- Step 4** In the Edit Dword Value window, click **Decimal**.
- Step 5** Modify the Cisco Unity comfort noise setting as needed (valid settings are 0 through 128):
- To decrease the volume of background noise between prompts and other audio, increase the setting (for example, to 60 dB). Make small adjustments to this setting of no more than 10 units.
 - To increase the volume of background noise, reduce the setting (for example, to 40 dB). Make small adjustments to this setting of no more than 10 units.
 - To disable Cisco Unity comfort noise, set the value to **128**.
- Step 6** Click **OK**.
- Step 7** Restart the Cisco Unity server.

Audio Troubleshooting Utilities

The following advanced audio utilities, which are available in the CommServer\Utilities\Audio directory, can be used to troubleshoot audio problems.

**Caution**

We recommend using these tools only with Cisco TAC supervision.

AudioStat

The AudioStat utility allows audio driver statistics to be viewed in real time. The information provided by the AudioStat utility can help isolate audio quality issues caused by packet delay and codec-related problems. Note that the current version of the AudioStat utility released with Cisco Unity version 4.0(3) requires version 7.0(3) of the Cisco Unity-CM TSP to properly display audio information.

Click the Global, Device, and Record Log tabs to display information, as shown in [Table 6-5](#), [Table 6-6](#), and [Table 6-7](#).

The Global tab displays information about the number of incoming and outgoing packets, RTP header errors, playback and recording counts, the number of out-of-sequence packets, and the number of times silence was inserted.

Table 6-5 AudioStat Utility Global Tab

Field Name	Description
G711 Packets G729 Packets	Number of incoming and outgoing G.711 and G.729a Real-Time Transport Protocol (RTP) packets. Note that packets are constantly being received, even if a recording is not in progress.
Other Packets	Number of other types of RTP packets sent and received, such as AVT tones or unknown audio formats received.
Out of Sequence	Number of packets received out of sequence.
RTP Header Errors	Number of RTP headers that were invalid.
Exceeded Silence Threshold	Usually indicates that silence was inserted by the audio driver, due to a missing packet. Note that a missing packet does not necessarily mean that there is a network issue. Some IP devices may not send any audio packets when the audio that would otherwise be sent is silence.
Playback Count and Record Count	Number of playbacks and recordings.

The Device tab displays the current status for each device. A red icon in the Device column indicates a recording in progress. When a recording ends, the data from that recording is displayed in the Record Log tab. To sort by a column, click the column heading.

Table 6-6 AudioStat Utility Device Tab

Field Name	Description
Device	Audio device number used for the recording. A red icon indicates a recording in progress.
State	Current activity.
Start Time	Time that the recording started.
End Time	Time that the recording ended.
Src IP Addr	Source IP address of the recording (for example, IP phone or gateway).
Src Port	Source port of the recording.
Codec	Recording format
Local Port	UDP port number used by Cisco Unity for the recording.
Duration	Length of the recording (in seconds).
Silence Inserted	Silence inserted in the recording (in seconds).

The Record Log tab displays a log of recording sessions. By default, the log is sorted by recording end time. To sort by a column, click the column heading. The Record Log Settings menu offers the following options for data collection and display:

- To change the maximum number of lines that are displayed in the Record Log window, click Settings > Options.
- To save the data in the Record Log window to an output file, click Settings > Logging, and then specify a file name and location.

Table 6-7 AudioStat Utility Record Log Tab

Field Name	Description
Device	Audio device number used for the recording.
Start Time	Time that the recording started.
End Time	Time that the recording ended.
Avg (ms)	Average time between packets (in milliseconds).
Src IP Addr	Source IP address of the recording (for example, an IP phone or gateway).
Src Port	Source port of the recording.
Codec	Recording format
Local Port	User Datagram Protocol (UDP) port number used by Cisco Unity for the recording.
Duration	Length of the recording (in seconds).
Silence inserted	Silence inserted in the recording (in seconds).

CAP Ripper

The CAP Ripper utility extracts RTP audio from .cap files created by Sniffer Pro or Network Monitor. Network Monitor (also known as NetMon) is a utility that comes with Microsoft Systems Management Server and Microsoft Windows 2000 Server. You use NetMon to capture and observe network traffic patterns and problems. For information on using NetMon, refer to the Microsoft Knowledge Base Article Q294818, available on the Microsoft Product Support website.

The CAP Ripper utility creates WAV files for each unique IP source and destination.

To Extract Audio by Using the CAP Ripper Utility

-
- Step 1** Create a .cap file containing RTP audio by using NetMon or Sniffer Pro.
- Step 2** Copy the .cap file to the \CommServer\Utilities\Audio directory on the Cisco Unity server.
- Step 3** At a command prompt, browse to the \CommServer\Utilities\Audio directory, and enter **capripper <Name of .cap file>**.

For example, enter **capripper capture1.cap**.

WAV file output is generated for each unique IP source/destination combination. For example:

```
Creating 10.93.248.235(31640) to 10.93.248.227(22818).wav
Creating 10.93.248.227(22816) to 10.93.248.235(31640).wav
```

- Step 4** Use the `-s` option to provide additional troubleshooting information about timing delays and sequencing of packets. For example, enter **capripper -s capture1.cap**.

The output shows detailed information from each of the WAV files. For example:

```
10.93.248.235(31640) to 10.93.248.227(22818).wav
RTP packets processed 275
Start seq 4881 End seq 5155
Format g729a
No packets out of sequence
Avg. time between packets 20.03ms
Longest packet delay 20ms
Total frames in .cap file 1433
```

- Step 5** If you receive the error message “No voice RTP packets found” when attempting to extract audio from a .cap file, verify that the capture file you are working with contains RTP packets.

If you are using a NetMon capture, and you are sure that the file contains RTP data, it may be possible that the starting offset of the capture data could not be determined. Use the `-d` option to view the binary data. For example, enter **capripper -d netmon.cap**.

A sample section of the output shows the following information:

```
000000A0 98 05 00 00 8D 7F 02 00 00 00 00 00 CE 01 00 00 .....
000000B0 00 00 00 00 00 00 00 00 29 04 00 00 00 00 00 .....).
000000C0 FF FF FF FF FF FF FF FF 00 00 00 00 FF FF FF FF .....
000000D0 FF FF FF FF 00 00 00 00 C8 4A 02 00 00 00 00 .....J.....
000000E0 3C 00 00 00 3C 00 00 00 FF FF FF FF FF FF 00 02 <...<.....
000000F0 A5 07 2A 18 08 06 00 01 08 00 ..*.....
```

- Step 6** To determine the starting offset, subtract 8 bytes from the first of two repeating DWORD values that you see in the .cap file. In the preceding example, the 3C value repeats on line E0. Note that the numbers in the file are in hex, and that there are 16 bytes displayed on each line. Eight bytes back from the first repeating DWORD value 0x3C is at 0x000000E0. Therefore, the starting offset of the first packet is $0xE0 - 8 = 0xD8$ or 216.

- Step 7** Indicate the starting offset obtained in [Step 6](#) with the `-o` option. For example, enter **capripper -o 216 netmon.cap**.

The output will show the delay and packet sequencing information.

RTP Parser

The RTP Parser add-on can be used to expand NetMon capability to decode RTP packets when viewing capture files in real time, or when viewing saved .cap files.

Network Monitor (also known as NetMon) is a utility that comes with Microsoft Systems Management Server and Microsoft Windows 2000 Server. You use NetMon to capture and observe network traffic patterns and problems. For information on using NetMon, refer to the Microsoft Knowledge Base Article Q294818, available on the Microsoft Product Support website.

To Install the RTP Parser

- Step 1** Copy the RtpParser.dll file from the CommServer\Utilities\Audio directory to the Winnt\System32\Netmon\Parsers directory on the Cisco Unity server.

Step 2 Restart NetMon.

To View a Capture File by Using the RTP Parser

Step 1 Create a .cap file containing RTP audio by using NetMon.

Step 2 View the .cap by file using NetMon Capture Summary View.

Step 3 Double-click on a frame row in the Summary View to see the RTP Parser View.



Message Waiting Indicators (MWIs)

This chapter describes message waiting indicators (MWIs), how they function in Cisco Unity, and methods for troubleshooting them.

How MWIs Function

An MWI is a lamp, flashing LCD panel, or special dial tone on subscriber phones that lets subscribers know a voice message is waiting. The type of indicator depends on the phone system and the phones that subscribers use.

MWIs are not the same as message notification, which is the feature that notifies a subscriber of new voice messages by calling a phone or pager, or by sending an e-mail message.

When MWIs Turn On and Off

There are two principal events that cause Cisco Unity to activate and deactivate MWIs:

- When a caller leaves a message for a subscriber, Cisco Unity notifies the phone system to activate the MWI on the phone for that subscriber.
- When the subscriber listens to the message, Cisco Unity notifies the phone system to deactivate the MWI on the phone.

There are two additional events that cause Cisco Unity to activate and deactivate MWIs:

- When a subscriber deletes a new message without listening to it or moves it to another folder, Cisco Unity notifies the phone system to deactivate the MWI on the phone.
- When MWIs are manually resynchronized—for example, by clicking **Resynchronize Now** on the **Properties** tab in the Cisco Unity Telephony Integration Manager (UTIM)—Cisco Unity queries the Data Object Hierarchy (DOH) to determine the status of MWIs on all phones and resets all MWIs.

However, an MWI remains activated under the following conditions when a subscriber listens to a new message:

- More messages are waiting to be heard. When all new messages are listened to, the MWI will be turned off.
- A new message arrives while the subscriber is listening to the original message. When all new messages are listened to, the MWI will be turned off.
- The subscriber listens on the phone to only part of the message and time stamp, then either hangs up or skips to the next message before hearing the entire message and time stamp.
- The server with the message store is offline and the message is stored in the Unity Messaging Repository (UMR).

- (Unified Messaging only) In the Inbox, the subscriber marks a listened-to message as unread.
- (Unified Messaging only) The subscriber uses the Inbox in offline mode to listen to messages.
- (Unified Messaging only) The subscriber uses the Lotus Notes client off line to listen to messages. Once the Lotus Notes client replicates with the Domino server, the MWI will be turned off.

In certain situations, MWIs are not activated:

- (Unified Messaging only) E-mail messages arrive. Cisco Unity monitors only voice messages.
- Fax messages arrive. Cisco Unity monitors only voice messages.
- (Unified Messaging only) Return receipts arrive. Cisco Unity monitors only voice messages.
- (Unified Messaging only) An Inbox rule automatically moves voice messages to another folder. Cisco Unity monitors only the Inbox.
- The server with the message store is offline and the message is stored in the UMR.
- (If a message store outage has occurred) After the offline message store has come back online, the messages that were stored in the UMR during the outage are moved to the message store, but MWIs will not be activated until you manually refresh them.

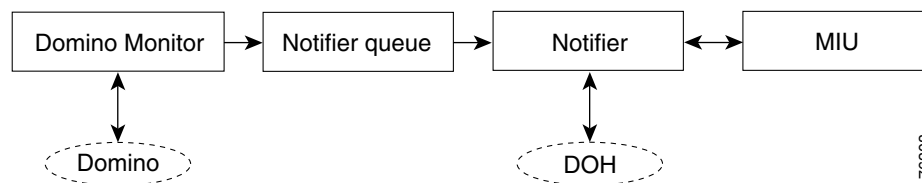
What Causes MWIs To Turn On and Off

The phone system is set up with one code or extension to turn MWIs on and a second code or extension to turn MWIs off. Cisco Unity sends the code or dials the extension to turn the MWI on and off for a subscriber.

You enter these codes or extensions in Cisco Unity in the Cisco Unity Telephony Integration Manager (UTIM)—click Programs > Cisco Unity > Unity Telephony Integration Manager.

Four Cisco Unity components (Domino Monitor, Notifier queue, Notifier, and Media Interface Unit or Miu) work together to turn MWIs on and off. [Figure 7-1](#) shows how these components interact.

Figure 7-1 Components That Turn MWIs On and Off



When a new message arrives in a subscriber Inbox, these components work together in the following sequence to activate the MWI on the phone of the subscriber:

1. The Domino Monitor receives DUCS notification from the Domino server each time a change occurs in the Inbox of each subscriber (when new voice messages arrive). When this happens, the Domino Monitor sends an MWI activation message to the Notifier queue.
2. The Notifier queue adds the MWI activation message as an MWI activation request (with the activation code or extension) to send to the phone system.
3. The Notifier queries the Data Object Hierarchy (DOH) to determine the status of the MWI on the phone of the subscriber.

If the DOH responds that the MWI is turned off, the Notifier sends the MWI activation request in the Notifier queue to the phone system.

If the DOH responds that the MWI is turned on, the Notifier discards the MWI activation request.

4. The Miu—which includes the integration—enables Cisco Unity to communicate successfully with the phone system. The phone system receives the request and activates the MWI on the phone of the subscriber.
5. The phone system sends the new status of the MWI (activated) to the Notifier, which then sends the status to the DOH where Cisco Unity records the MWI status.

When there are no more new messages in the subscriber Inbox (all new messages have been listened to, deleted, or marked as read), the same four Cisco Unity components work together in the following sequence to deactivate the MWI on the phone of the subscriber:

1. The Domino Monitor receives DUCS notification from the Domino server each time a change occurs in the Inbox of each subscriber (all voice messages are listened to, deleted, or marked as read). When this happens, the Domino Monitor sends an MWI deactivation message to the Notifier queue.
2. The Notifier queue adds the MWI deactivation message as an MWI deactivation request (with the deactivation code or extension) to send to the phone system.
3. The Notifier queries the DOH to determine the status of the MWI on the phone of the subscriber.
If the DOH responds that the MWI is turned on, the Notifier sends the MWI deactivation request in the Notifier queue to the phone system.
If the DOH responds that the MWI is turned off, the Notifier discards the MWI deactivation request.
4. The Miu—which includes the integration—enables Cisco Unity to communicate successfully with the phone system. The phone system receives the request and deactivates the MWI on the phone of the subscriber.
5. The phone system sends the new status of the MWI (deactivated) to the Notifier, which then sends the status to the DOH where Cisco Unity records the MWI status.

What Causes MWIs to Behave Differently Than Expected

The following conditions cause MWIs to behave differently than expected:

- (Unified Messaging only) An Inbox rule automatically moves voice messages to another folder. Cisco Unity monitors only the Inbox, so the MWI is not activated.
- The DOH, which records the status of the MWI for each subscriber, received an indication that an activation or deactivation request had not succeeded when in fact it had. Consequently, the Notifier may discard subsequent MWI requests.
- There are an inadequate number of voice messaging ports on the Cisco Unity server resulting in the ports not being immediately available to dial out for activating and deactivating MWIs.
- An inadequate number of voice messaging ports on the Cisco Unity server are set to Dialout MWI, resulting in the ports being too busy to dial out immediately to activate and deactivate MWIs.
- No voice messaging ports on the Cisco Unity server are enabled to dial out.
- (Multiple Cisco CallManager clusters) There are no voice messaging ports on the Cisco Unity server dedicated to activating and deactivating MWIs. There should be one port dedicated to each cluster.
- (Cisco CallManager) In the UTIM, the MWI On Extension and MWI Off Extension fields on the MWI tab do not have the extensions that the phone system requires.
- (Circuit-switched phone systems) In UTIM, the MWI On Code and MWI Off Code fields on the MWI tab do not have the code that the phone system requires.
- The codes or extensions are switched (for example, the code that activates MWIs is entered in the MWI Off Code field).

- (Cisco CallManager) The extensions that activate and deactivate MWIs are not in the same calling search space that contains the phones and voice mail ports.
- The subscriber may not have the correct phone system assignment set on the Subscribers > Subscribers > Profile page.
- MWIs are not enabled for the subscriber on the Subscribers > Subscribers > Messages page.
- The wrong extension for the subscriber is entered in the Extension field on the Subscribers > Subscribers > Messages page.
- The Domino server is shut down or is off line.
- The phone system is programmed to send calls to a voice messaging port on the Cisco Unity server that sets MWIs but does not answer calls.
- (Cisco CallManager) A route plan (or dial plan) overlaps with an MWI extension number, so while the phone system waits for additional digits, Cisco Unity abandons the MWI request and the DOH records that the request failed. The phone system then successfully completes the MWI request.
- (Serial integrations) A faulty RS-232 serial cable passes data from the phone system to Cisco Unity but not from Cisco Unity to the phone system. The result is that Cisco Unity sends MWI requests to the phone system, but the phone system does not receive them.
- When a Lotus Domino user is imported into Cisco Unity, the ownership information is used for MWI functionality. Occasionally, Lotus Domino incorrectly sets the Owner field on the voice message file for a Cisco Unity subscriber, so MWIs will not be activated or deactivated for the subscriber.

Troubleshooting MWIs When They Do Not Turn On or Off

To troubleshoot MWIs when they do not turn on or off, do the procedures for the following components in the order given:

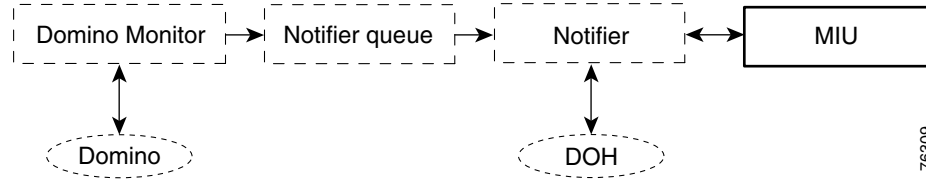
- [Miu Component, page 7-4](#)
 - [Resolving Cisco CallManager Integration Problems, page 7-7](#)
 - [Subscriber Phone System Assignment Is Incorrect, page 7-8](#)
- [Notifier and Notifier Queue Components, page 7-8](#)

Miu Component

This section describes troubleshooting the Miu component, which includes the integration. Many MWI problems can be resolved by troubleshooting this component. In addition, if MWI requests reach the Miu, the components that handle MWIs before the Miu probably are processing MWIs correctly.

[Figure 7-2](#) shows the focus.

Figure 7-2 Miu Component in the Troubleshooting Process



76309

Do the following procedures in the order given.

To Verify Phone System and Port Settings in UTIM

-
- Step 1** On the Windows Start menu of the Cisco Unity server, click **Programs > Cisco Unity > Unity Telephony Integration Manager**. UTIM appears.
- Step 2** In the left pane, click the applicable integration.
- Step 3** In the right pane, click the **MWI** tab.
- Step 4** Confirm that the codes or extensions to activate and deactivate MWIs are correct:
- (Circuit-switched phone systems) In UTIM, the values for the **MWI On Code** and **MWI Off Code** fields match the codes the phone system uses.
 - (Cisco CallManager) In UTIM, the values in the **MWI On Extension** and **MWI Off Extension** fields match the extensions the phone system uses.
- Step 5** If you changed any settings, click **Save**.
- Step 6** Click the **Ports** tab.
- Step 7** Confirm that the correct port ranges have been assigned to the applicable phone system.
- Step 8** If you changed any settings, click **Save**.
- Step 9** Confirm the settings on the remaining tabs.
- Step 10** Exit UTIM. If prompted, restart the Cisco Unity services.
-

To Confirm That MWIs Are Enabled for the Subscriber

-
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Messages** page for the subscriber.
- Step 2** Confirm that the **Use MWI for Message Notification** check box is checked.
- Step 3** Confirm that the MWI Extension field is set to X (indicating the primary extension assigned to a subscriber) or to the extension number on which MWIs will be set for the subscriber.
-

To Set the Subscriber Ownership for a Lotus Domino Voice Message File

When an IBM Lotus Domino user is imported into Cisco Unity, the ownership information is used for MWI and message notification functionality. Occasionally, Lotus Domino incorrectly sets the Owner field on the mail file for a Cisco Unity subscriber, so MWIs and message notification will not be activated or deactivated for the subscriber.

-
- Step 1** In the Lotus Notes client, open the mail file of the subscriber.
 - Step 2** On the Tools menu, click **Preferences**.
 - Step 3** Under User Configuration, in the This Mail File Belongs To list, click the Cisco Unity subscriber name.
 - Step 4** Click **OK**.
 - Step 5** Close the mail file.
-

To Confirm That the Miu Allows Cisco Unity and the Phone System to Communicate

-
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
 - Step 2** Set up message notification for urgent messages for the subscriber.
 - Step 3** Send an urgent message to the subscriber. If message notification of the urgent message arrives, the problem with MWIs is probably caused by the integration. Continue with the following “[To Troubleshoot Miu Problems](#)” procedure.
-

To Troubleshoot Miu Problems

-
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscriber > Messages** page.
 - Step 2** Confirm that the Use MWI for Message Notification check box is checked and that the Extension field is either **X** (which causes Cisco Unity to use the MWI on the subscriber extension) or the actual subscriber extension.
 - Step 3** Browse to the \Commsvr\TechTools\ directory and double-click **StatusMonitor.exe**.
 - Step 4** In the Status Monitor window, confirm that the Display check box is checked, and click **Start All Monitors**.
 - Step 5** Go to the **Subscribers > Subscriber > Messages** page, and click **Resynchronize MWIs**. In the Status Monitor window, the following message should appear:
“Dialing” (MWI) 'X'
 - MiuGeneral—0–4, 12, 16
 - MiuIO—11, 14
 - Step 6** If the message appears, the MWIs are resynchronized and function correctly. Skip the rest of this procedure.
If the message does not appear, on the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.
 - Step 7** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon.
 - Step 8** Set the following diagnostic traces:
 - MiuGeneral—0–4, 12, 16
 - MiuIO—11, 14

- MiuMethods—10, 12, 14, 18
- (Circuit-switched phone systems) MiuMethods—20, 22
- MiuIntegration—12

Step 9 On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.

Step 10 Leave a message for a subscriber.

Step 11 Review the diagnostic logs to determine the cause of the problems.



Note The command SetMWI is the one that is used by the Miu to set the MWI on a phone.

Step 12 On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.

Step 13 In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.

Resolving Cisco CallManager Integration Problems

Consider the following issues if Cisco CallManager is integrated with Cisco Unity:

- The unique extensions for turning MWIs on and off may not have been entered in the Cisco CallManager server, or the Cisco CallManager server has not been restarted to enable these values. For instructions on setting these extensions, refer to the applicable Cisco CallManager integration guide.
- A Cisco CallManager route plan may include the unique extensions for turning MWIs on and off. For example, a route plan could send all numbers starting with 9 to a gateway, while the extension that turns MWIs on is 99991. Revise the route plan so it does not include the MWI extensions or alter the extensions. For instructions on setting up route plans, refer to the applicable *Cisco CallManager Administration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- The unique extensions for turning MWIs on and off may not have been entered in the MWI On Extension and MWI Off Extension fields in UTIM, or Cisco Unity may not have been restarted to enable these values. Enter the applicable values in UTIM. For instructions on setting these values in UTIM, refer to the applicable Cisco CallManager integration guide.
- The IP phone may not be in the same calling search space and partition as the Cisco Unity voice messaging ports. From a phone, dial the extension that turns on MWIs. If you hear the reorder tone, the extension for turning MWIs on is not assigned the correct calling search space and partition in Cisco CallManager. If you do not hear the reorder tone but the MWI is not activated or deactivated, a route plan may be causing the problem.
- The unique extensions for turning MWIs on and off in Cisco CallManager may not be identical to the values entered in the MWI On Extension and MWI Off Extension fields in UTIM. Confirm the values and restart the Cisco CallManager servers and Cisco Unity server. For instructions on setting these values, refer to the applicable Cisco CallManager integration guide.
- If the site has a publisher (primary) and subscriber (secondary) Cisco CallManager server, the unique extensions for turning MWIs on and off may not have been set on the subscriber Cisco CallManager server, or the subscriber CallManager server may not have been restarted to enable these values. On the subscriber Cisco CallManager server, set the extensions for turning MWIs on and off, and restart the Cisco Unity server. For instructions on setting these extensions, refer to the applicable Cisco CallManager integration guide.

- If Cisco Unity integrates with multiple Cisco CallManager clusters, you need to dedicate at least one voice messaging port to set MWIs for each cluster. For example, in a two-cluster environment, there must be at least two ports dedicated to setting MWIs, one sending MWI requests for the first cluster and another sending MWI requests to the second cluster. Confirm that at least one voice messaging port is dedicated to each cluster and that the port is set to Dialout MWI. For instructions on configuring ports, refer to the applicable Cisco CallManager integration guide.

The Cisco CallManager integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.

Subscriber Phone System Assignment Is Incorrect

If the subscriber is assigned to the wrong phone system, do the following procedure.

To Confirm the Subscriber Phone System Assignment (Dual Phone System or Former Dual Phone System Integration)

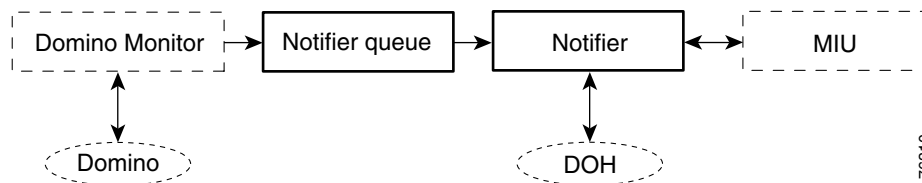
-
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page.
- Step 2** In the Subscriber Information section, confirm that the correct phone system has been selected for the subscriber. Correct if necessary.
- Step 3** If you made a change, click **Save**, then shut down and restart Cisco Unity.
-

Notifier and Notifier Queue Components

If the Miu component does not receive MWI requests, the problem lies earlier in the MWI process. This section describes troubleshooting the Notifier and Notifier queue components.

If MWI requests reach the Notifier queue and the Notifier components, the Domino Monitor component is probably processing MWIs correctly. [Figure 7-3](#) shows the focus.

Figure 7-3 Notifier and Notifier Queue Components in the Troubleshooting Process



Do the following procedures in the order given.

To Confirm That the Notifier Makes MWI Requests

-
- Step 1** On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 2** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.
- Step 3** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon.
- Step 4** Check the check boxes for Notifier—12 and 20.

- Step 5** On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.
- Step 6** Leave a message for a subscriber.
- Step 7** To view the log files, click **Processes > AvCsMgr**, and then click the **Current** log file.
- Step 8** The selected log file is formatted and appears in the right pane.
- Step 9** Check the log for the following:
- A Notifier—12 entry with the correct subscriber and extension listed to confirm that the MWI request is made with the correct information.
 - The entry contains the text “Queued MWI task for mailuser.”
- Step 10** If the Notifier thinks the MWI is already activated, the Notifier does not make the MWI request. In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Messages** page for the subscriber. Then click **Resynchronize MWIs**.

To Confirm That MWI Requests Are Successful

- Step 1** In the log from the preceding procedure, locate a Notifier—12 entry.
- Step 2** If the entry has the text “Completed MWI task for mailuser,” the MWI request was successful. If not, depending on the content of the entry, do one of the following:
- If the entry has the text “Received: Task” or “Continues Task,” the MWI request was not successful. Check the diagnostic log for any problem with the voice messaging ports. See the procedure [To Troubleshoot Port Problems, page 7-9](#).
 - If the diagnostic log indicates the MWI request was successful, but the MWI is not activated, set diagnostic traces for Notifier—12, MiuIntegration—12, and MiuMethods—20, 21, and review the logs.
- Step 3** On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 4** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.

Do the following procedure as needed.

To Troubleshoot Port Problems

- Step 1** In the Cisco Unity Administrator, go to the **System > Ports** page, and confirm that some ports are set to **Dialout MWI**.
For dual phone system integrations, make sure that each phone system has some of its ports set to **Dialout MWI**.
- Step 2** On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.
- Step 3** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.
- Step 4** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon.
- Step 5** Set the following diagnostic traces:
- Notifier—20
 - Arbiter—13

- ResourceManager—12

Step 6 On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.

Step 7 Leave a message for a subscriber.

Step 8 Review the diagnostic logs to determine the cause of the problems.

Step 9 On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon.

Step 10 In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.

Troubleshooting MWIs When They Are Delayed Turning On and Off

There are several possible reasons that MWIs may be delayed turning on and off. These reasons include:

- [Cisco Unity Domino Server Is Down or Is Disconnected, page 7-10](#)
- [Ports Are Too Busy to Turn MWIs On and Off Promptly, page 7-10](#)
- [Not Enough Ports Are Set for MWIs, page 7-11](#)
- [Calls Are Sent to Cisco Unity Ports That Set MWIs but Do Not Answer Calls, page 7-11](#)

Cisco Unity Domino Server Is Down or Is Disconnected

Messages recorded while the Domino server (the message store) is down or disconnected are stored in the Unity Messaging Repository (UMR) until the server is brought back up. Because MWIs are not lit until a message is actually delivered to a subscriber, the delay experienced between the time a message is recorded and its delivery and the lighting of the MWI is entirely dependant on the amount of time that the message store was down or disconnected.

Ports Are Too Busy to Turn MWIs On and Off Promptly

When the ports that turn MWIs on and off are also set to perform other operations, they may be too busy to turn MWIs on and off promptly. You can improve MWI performance by taking the following actions:

- Dedicate a number of ports exclusively to turning MWIs on and off.
- Make sure that the entry point of the Cisco Unity hunt group for ports is not a port that also handles MWIs.
- Use the last ports assigned to a phone system to turn MWIs on and off.
- For systems that handle a large volume of calls, install additional ports.

To Review Port Configuration for Message Waiting Indication (Non-Serial Integrations Only)

Step 1 In the Cisco Unity Administrator, go to the **System > Ports** page.

- Step 2** Review the existing port configuration and determine if one or more ports can be set only to **Dialout MWI**.
-

Not Enough Ports Are Set for MWIs

When Cisco Unity takes a lot of messages, the ports assigned to turn MWIs on and off may not always be able to dial out promptly. A single port set to dial out only for Message Waiting Indication with an IP phone system integration can change approximately 240 to 360 MWIs per hour, depending on the phone system. An analog integration can take up to seven seconds per MWI change.

If the percentage of ports used does not exceed 40 percent usage during peak periods, then the number of message waiting indication ports is adequate. If the percentage of ports used exceeds 40 percent usage during peak periods, review the existing port configuration and determine if one or more additional ports can be set only to Dialout MWI.

To Determine Whether the Number of Message Waiting Indication Ports Is Adequate

- Step 1** On the Cisco Unity server 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** Run the Port Availability report. You may also find the Port Time Use report helpful.
- Step 4** If the percentage of ports used exceeds 40 percent usage during peak periods, go to the **System > Ports** page in the Cisco Unity Administrator, then continue with [Step 5](#).
- If the percentage of ports used does not exceed 40 percent usage during peak periods, the number of message waiting indication ports is adequate.
- Step 5** Review the existing port configuration and determine if one or more additional ports can be set only to **Dialout MWI**.
-

Calls Are Sent to Cisco Unity Ports That Set MWIs but Do Not Answer Calls

If the phone system is programmed to send calls to a port on Cisco Unity that is configured to set MWIs and not to answer calls, MWIs may be delayed.

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

- Step 1** In the Cisco Unity Administrator, go to the **System > Ports** page.
- Step 2** Note which ports are designated to answer calls.
- Step 3** In the phone system programming, confirm that calls are only being sent to ports designated to answer calls.
- Step 4** If you make a change to the phone system programming, shut down and restart the Cisco Unity server to clear any hung ports.
-

Troubleshooting MWIs When They Sometimes Do Not Turn Off

There is one possible reason for MWIs not turning off as expected.

MWIs Have Lost Synchronization

MWIs may lose synchronization if, for example, the phone system is off-line when an MWI status changes.

Do the following procedure.

To Resynchronize MWIs

-
- Step 1** On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. UTIM appears.
 - Step 2** For the integration node, click the **Properties** tab.
 - Step 3** In the MWI Synchronization section, click **Resynchronize Now**.
 - Step 4** If applicable, check the Resynchronize At check box, and choose the time that you want the system to resynchronize the MWIs. We recommend choosing a time outside of regular business hours because of the Cisco Unity resources needed for resynchronization.
-

Additional References

More information about setting up MWIs can be found in the following documents:

- Cisco Unity integration guides for various phone systems available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.
- *Cisco Unity System Administration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.
- *Cisco Unity Release Notes* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/relnote/cu403rn.htm.



Message Notification Calls

About Problems with Message Notification Calls

Problems with message notification calls that Cisco Unity makes to a subscriber pager, or a work, home, or spare phone fall into two categories:

Message notification is slow	When multiple subscribers report that message notification is slow, a port setup problem is the likely cause. See the “Message Notification Is Slow for Multiple Subscribers” section on page 8-1. Isolated complaints about slow message notification likely are related to a subscriber message notification settings. See the “Message Notification Is Slow for a Subscriber” section on page 8-3.
Message notification does not work at all	Some system problems can prevent Cisco Unity from making any notification calls. See the “Message Notification Calls Are Not Made to Any External Numbers” section on page 8-5. When a subscriber sets up message notification incorrectly, it can prevent Cisco Unity from making any notification calls to that subscriber. See the “Message Notification Is Not Working at All for a Subscriber” section on page 8-5.

Message Notification Is Slow for Multiple Subscribers

There are several possible reasons that message notification may appear to be slow for multiple subscribers. Use the [“Task List for Troubleshooting Slow Message Notifications for Multiple Subscribers”](#) to troubleshoot the possible causes.

Task List for Troubleshooting Slow Message Notifications for Multiple Subscribers

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 8-2.
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 8-2.
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 8-2.
4. Confirm that the Domino server is not down or disconnected. See the [“Cisco Unity Domino Server Is Down or Is Disconnected”](#) section on page 8-3.

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 the Cisco Unity Administrator, go to the **System > Ports** page.
 - Step 2** Review the existing port configuration and determine if 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 takes a lot of messages, the notification ports may not always be able to dial out promptly.

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

If the percentage of ports used does not exceed 70 percent usage during peak periods for the ports set to dial out for message notification, the number of notification ports is adequate. Contact the Cisco Technical Assistance Center (TAC) to resolve the problem.

To Determine Whether the Number of Message Waiting Indication Ports Is Adequate

-
- Step 1** On the Cisco Unity server 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** Run the Port Availability report. You may also find the Port Time Use report helpful.
 - Step 4** If the percentage of ports used exceeds 40 percent usage during peak periods, go to the **System > Ports** page in the Cisco Unity Administrator, then continue with [Step 5](#).
If the percentage of ports used does not exceed 40 percent usage during peak periods, the number of message waiting indication ports is adequate.
 - Step 5** Review the existing port configuration and determine if 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 that is not configured to answer calls, Cisco Unity will not answer the call.

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

- Step 1** In the Cisco Unity Administrator, go to the **System > Ports** page.
 - 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 Cisco Unity server to clear any hung ports.
-

Cisco Unity Domino Server Is Down or Is Disconnected

Messages recorded while the Domino server (the message store) is down or disconnected are stored in the Unity Messaging Repository (UMR) until the server is brought back up. Because calls for message notification are not made until a message is actually delivered to a subscriber, the delay experienced between the time a message is recorded and its delivery and the sending of the notification is entirely dependant on the amount of time that the message store was down or disconnected.

Message Notification Is Slow for a Subscriber

There are several possible reasons that message notification may appear to be slow for a subscriber. Use the [“Task List for Troubleshooting Slow Message Notification for a Single Subscriber”](#) to troubleshoot the possible causes.

Task List for Troubleshooting Slow Message Notification for a Single Subscriber

1. The subscriber settings may not be adequate for the needs of the subscriber. See the [“Message Notification Setup Is Inadequate”](#) section on page 8-3.
2. The subscriber settings may need adjustment to more correctly map to the work schedule of the subscriber. See the [“Notification Attempts Are Missed”](#) section on page 8-4.
3. The subscriber may not clearly understand how repeat notifications are handled by Cisco Unity. See the [“Repeat Notification Option Is Misunderstood”](#) section on page 8-4.

Message Notification Setup Is Inadequate

When a subscriber 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 the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
- Step 2** In the Device list, click the correct notification device.

- Step 3** Confirm with the subscriber that the notification device is applicable to the needs of the subscriber. If the subscriber has selected a very busy phone for Cisco Unity to call, ask if there is an alternate phone or pager to use for message notification.
 - Step 4** Confirm with the subscriber that the notification schedule is consistent with the days and times that the subscriber is available to receive notification calls.
-

Notification Attempts Are Missed

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

To Resolve Missed Notification Attempts

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
- Step 2** In the Device list, click the correct notification device.
- Step 3** In the Notification Options section, check the **Restart Notification Each Time a New Message Arrives** check box.
- Step 4** In the Try Again How Many Times boxes, increase the numbers so that Cisco Unity makes more notification calls when the device does not answer or is busy.
- Step 5** In the How Many Minutes To Wait Between Tries boxes, decrease the numbers so that Cisco Unity makes notification calls more often when the device does not answer or is busy.
- Step 6** In the If Notification Fails box, select **Pager** as a backup device if the subscriber has a pager available for use. Also enter settings and a schedule for the pager.
- Step 7** Suggest that the subscriber set up an answering machine for the notification phone, so that notification calls are received even when the subscriber is unavailable.

When Cisco Unity is set to call a phone that has an answering machine, confirm with the subscriber 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 to repeat notification at a particular interval when there are still new messages can be useful for subscribers who receive a lot of messages but who do not want immediate notification. However, when a subscriber chooses not to have Cisco Unity restart notification each time a new message arrives, setting a long interval between repeat notification calls may lead the subscriber to believe that Cisco Unity is delaying notification.

To Resolve a Repeat Notification Problem

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.

- Step 2** In the Device list, click the correct notification device.
- Step 3** In the Notification Options section, in the box next to the Repeat Notification If There Are Still New Messages After This Many Minutes check box, set a shorter interval, such as **15** minutes.
-

Message Notification Calls Are Not Made to Any External Numbers

A possible cause for this problem is that Cisco Unity cannot access an external line.

To Verify External Line Access (Circuit-Switched Phone Systems Only)

- Step 1** 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 1-1.
- Step 2** On Phone 1, dial the access code necessary to get an external line.
- Step 3** Dial an external phone number.
- If you do not reach the external number, continue with [Step 4](#).
- If you reach the number, Cisco Unity can access external lines for message notification. Message notification settings in the subscriber template may be preventing Cisco Unity from making notification calls. Verify the message types and access code in the template, and change the values if necessary. If you make changes to the template message types or access code, you must make the same changes to all existing subscriber accounts based on the subscriber template.
- Step 4** Review the phone system programming for restrictions on external line access. Change the phone system programming values as necessary, and repeat the test.
- If the test fails again, contact Cisco TAC.
-

Message Notification Is Not Working at All for a Subscriber

There are several possible reasons that message notification may not work at all for a subscriber. Use the [“Task List for Troubleshooting Non-Functional Message Notifications for a Subscriber”](#) to troubleshoot the possible causes.

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

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 8-6.
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 8-6.
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 8-6.

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 8-7.

Only Certain Types of Messages Are Set to Trigger Notification

Cisco Unity can be set so that a subscriber is notified only of certain types of messages. For example, if subscriber notification is set up only for fax and urgent voice messages, e-mail and regular voice messages will not cause Cisco Unity to make a notification call.

To Change the Message Types That Trigger Notification Calls

-
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
 - Step 2** In the Device list, click the correct notification device.
 - Step 3** In the Notify Subscriber Of section, verify the selected message types with the subscriber.
-

Access Code for an External Line Is Missing

To place an external call, a subscriber usually must dial an access code to get an external line (for example, 9). When the phone system requires an access code, an external message notification phone number set in Cisco Unity 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 the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
 - Step 2** In the Device list, click the correct notification device.
 - Step 3** 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 subscriber may have entered a wrong phone number for Cisco Unity to call. Also, when a subscriber disables notification to a phone or pager, Cisco Unity 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 the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
 - Step 2** In the Device list, click the correct notification device.
 - Step 3** In the Phone Number box, confirm that the correct access code and phone number are entered for the device.
 - Step 4** In the Status section, confirm that the device is set to **Enabled**.
-

To Test a Notification Device

- Step 1** If the notification device is a cellular phone or pager, ask the subscriber to have it available for the test. If the notification device is a home phone or another phone away from the office, ask the subscriber 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 1-1.
 - Step 4** On Phone 1, dial the notification number set in Cisco Unity for the device.

If the pager is activated or the phone rings, you have confirmed that Cisco Unity 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 subscriber 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 the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page for the subscriber.
 - Step 2** In the Notification Options section, note the phone system assigned to the device in the Switch field at the bottom of the page.
 - Step 3** Go to the **System > Ports** page for the phone system assigned to the device.
 - Step 4** 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 5** Click the **Save** icon.
-

■ Message Notification Is Not Working at All for a Subscriber



Hardware

About Problems with Hardware

Problems with the Cisco Unity server itself, or with required or optional third-party hardware can include:

Network Interface Card problems	See the “Network Interface Card Problems” section on page 9-1.
Voice card problems	See the “Voice Cards Incorrectly Reported As New Hardware or Missing Drivers” section on page 9-3.

Network Interface Card Problems

There are several possible reasons that problems can arise when using a Network Interface Card (NIC) on a Cisco Unity server. See the following topics to troubleshoot problems related to NIC configuration:

- [Cisco Unity Plays System Prompts but Does Not Transmit Voice, page 9-1](#)
- [CreateUser Errors Occur During a False Network Disconnect, page 9-2](#)

Cisco Unity Plays System Prompts but Does Not Transmit Voice

If callers can hear Cisco Unity prompts, but Cisco Unity does not transmit any audio when a caller speaks, Cisco Unity may have a dual NIC misconfiguration.

When dual NICs in a Cisco Unity system are configured with separate interface IP addresses, this may prevent correct receipt of RTP packets for voice transmissions. You can find this problem recorded in the log and trace files as silence detection filtering because Cisco Unity is not receiving any audio, and the wave driver is reporting silence detection on all recordings. This problem may also occur when a second NIC is installed in the Cisco Unity server but is not configured or connected to the network.

When dual NICs are installed on a Cisco Unity server, both NICs must be configured to share the same IP address.

To confirm or change NIC configuration settings, do the procedure in the [“Configuring Dual NICs”](#) section on page 9-2.

CreateUser Errors Occur During a False Network Disconnect

When doing a bulk addition of a large number of Cisco Unity subscribers, random CreateUser errors may be generated. In a test situation, the error message “ERROR 800406ba: CreateUser()” was received for approximately 4 out of every 1000 subscribers successfully added.

The error messages refer to losing the network connection. However, it can be verified that the network connections are not actually disconnected. The cause can instead be traced to dual NICs on the Cisco Unity server, where the server was randomly trying to access one or the other card, and subsequently reported a network disconnect.

To resolve this problem, dual NICs on a Cisco Unity server must be configured with one NIC designated as the primary, and the other as secondary. The NICs must be configured in adapter fault tolerant mode (AFT) or network fault tolerant (NFT) mode only. Virtual adapter configuration mode is not supported with dual NICs on a Cisco Unity server.

To confirm or change NIC configuration settings, do the procedure in the [“Configuring Dual NICs” section on page 9-2](#).

Configuring Dual NICs

When dual NICs are installed on a Cisco Unity server, they must be properly configured or a variety of problems can occur.

If the Cisco Unity server is using dual NICs, we recommend that they be configured in AFT or NFT mode. One NIC is designated as the primary and the other NIC as the secondary for active-passive fault tolerance. In this configuration, the primary (active) NIC handles 100 percent of the traffic. Only in the event that the primary NIC becomes unavailable does the secondary NIC then become active and handle 100 percent of the traffic.

Alternatively, if you do not want to configure AFT or NFT, or do not have a second LAN port available, the following configurations are supported, though not recommended:

- Disable TCP/IP for the second NIC, which allows you to re-enable the second NIC remotely if the first NIC fails. (Use the Network and Dial-up Connections Control Panel to disable TCP/IP for the second NIC.)
- Disable the second NIC in the BIOS.



Caution Note that it is not sufficient simply to refrain from plugging a network cable into the second NIC. The NIC must be disabled in the BIOS, or Cisco Unity may not work properly.

To confirm or change NIC configuration settings, do the following procedure.

To Confirm or Change Dual NIC Configuration on a Cisco Unity Server

Step 1 Confirm that the NICs are configured correctly:

- Both are connected to the same network segment.
- Both share the same IP address.
- Both are set up for AFT when using a Dell or IBM server, or for NFT when using a Hewlett-Packard server. (Refer to the documentation provided by the NIC manufacturer or server vendor. If you are configuring an MCS-7825H, MCS-7835H, or MCS-7845H server, configure NFT teaming by using the network teams property sheet of the Compaq Network Teaming and Configuration Utility

(CPQNTAC). If you are configuring an MCS-7815I, MCS-7855I, or MCS-7865I server, configure AFT teaming by using the Advanced Control Suite of the Broadcom NetXtreme Ethernet utilities. For the MCS-7835I and MCS-7845I servers, configure AFT teaming by using the teaming wizard on the Advanced tab of the Intel PROSet II Ethernet utilities.)

Step 2 Restart the Cisco Unity server for any changes to take effect.

Voice Cards Incorrectly Reported As New Hardware or Missing Drivers

In the following cases, the Found New Hardware wizard may appear each time the Cisco Unity server is restarted and report that the voice cards are new hardware, even though the cards are properly installed and configured:

- The operating system was installed by using the Platform Configuration discs.
- The operating system was installed by using the manufacturer's guided system-setup utility before the voice cards were installed.
- New voice cards were added to an existing Cisco Unity server.

Do the procedure in this section to prevent the Found New Hardware wizard from reporting the voice cards as new hardware. The procedure will not prevent the Found New Hardware wizard from finding and reporting other new hardware.

We recommend disabling virus-scanning services, if applicable, for the duration of the procedure, because running the services slows the Found New Hardware wizard. Re-enable the services when you are finished.

To Disable the Found New Hardware Wizard for the Voice Cards

- Step 1** On the Found New Hardware wizard Welcome page, click **Next**. (After the Cisco Unity server is restarted, the Found New Hardware wizard Welcome page is displayed along with the PCI Device Installing dialog.)
- Step 2** On the Install Hardware Device Drivers page, click **Search for a Suitable Driver for My Device (Recommended)**, and click **Next**.
- Step 3** On the Locate Driver Files page, check the **Floppy Disk Drives** and **CD-ROM Drives** check boxes, and click **Next**.
- Step 4** On the Driver Files Search Result page, click **Disable the Device**, and click **Finish**. Do not choose to skip driver installation of this device, or the Found New Hardware wizard will continue to appear each time the Cisco Unity server is restarted.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each instance of the Found New Hardware wizard (for each voice card, as applicable).

Note that doing this procedure does not prevent a voice card from being displayed as an unknown PCI device when viewed in the Windows 2000 Device Manager. The warning that the device drivers are not installed also will continue to be displayed. This is expected behavior, and does not indicate a problem with the card or with the Cisco Unity server.



Error Messages

About Error Messages

Error message problems fall into these categories:

Startup error messages	These are error messages that may appear when Cisco Unity or the Cisco Unity server is started. See the “ Startup Error Messages ” section on page 10-1.
Browser and Windows error messages	Browser error messages may appear when subscribers attempt to log on to the Cisco Unity Administrator or the Cisco Personal Communications Assistant (PCA). Windows error messages may appear when you access Administrative Tools. See the applicable section: <ul style="list-style-type: none">• Cisco Unity Administrator Browser Error Messages and Windows Error Messages, page 10-3.• Cisco PCA Error Messages, page 15-8.
E-mail and voice error messages	Cisco Unity may send e-mail and voice mail error messages. See the “ E-Mail and Voice Error Messages ” section on page 10-5.
Media Master error messages	These are error messages that may appear when subscribers use the Media Master control bar in the Cisco Unity Administrator or the Cisco Unity Assistant. See the “ Procedures for Troubleshooting the Media Master Control Bar ” section on page 15-9.

For information about the error messages that Cisco Unity writes to the Windows Application Event log, refer to <http://www.CiscoUnitySupport.com>.

Startup Error Messages

Use the information in this section to troubleshoot errors that occur when starting either the Cisco Unity software or server.

Cisco Unity Fails to Start

Error Message At least one service or driver failed during system startup.

Explanation This message is displayed when one or more of the Cisco Unity services or the services required by Cisco Unity do not start.

Recommended Action To troubleshoot this problem:

- Check the startup settings for the services as described in the procedure [To Check the Service Startup Settings, page 10-2](#).
- Check for errors listed in the Application and System Event logs as described in the procedure [To Look for Errors in the Application and System Event Logs, page 10-2](#).

To Check the Service Startup Settings

Do the steps below for each of the following services:

- These Cisco Unity services: AvCsGateway and AvCsMgr
- Dialogic
- IIS Admin Service
- World Wide Web Publishing Service

-
- Step 1** In the Control Panel Services dialog box, click the service, then click **Startup**.
- Step 2** Verify that Manual is selected for AvCsMgr, AvUMRSyncSvr, AvRepDirSvrSvc, and Remote Access Connection Manager.
- Step 3** Verify that Automatic is selected for the other services.
- Step 4** Verify that the domain name, user name, and password in the account assigned to the service are correct and that the account has the correct rights and permissions as shown in the following table:
- Step 5** If the Remote Access Connection Manager service is started, stop the service, then restart Cisco Unity.
-

To Look for Errors in the Application and System Event Logs

Because startup events occur in rapid succession, when you look in the Application or System Event log for information about these events, you will be looking for the first event in a series of events that probably occurred just seconds apart. Locate the first error in the startup attempt. Subsequent errors may have been caused by the first error. If you can determine the cause and fix the first error, then shut down and restart the Cisco Unity server. All subsequent errors may be resolved by fixing the first.

-
- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.
- Step 2** In the Application Event log, look at the Date and Time columns to find the first event in the current startup attempt.
- Step 3** When you find the first event in the startup attempt, look for the first error that occurred after it. If no errors appear in the startup attempt, skip to [Step 5](#).
- Step 4** Look at the value in the Source column for the first error and then for any subsequent errors in the startup attempt.

If the name in the source begins with “CiscoUnity” or with the letters “Av,” double-click the error to display a dialog box containing additional information that may help you solve the problem.

If the Source column for an error contains any other value, or if you cannot determine the cause of the problem, contact the Cisco Technical Assistance Center (TAC).

Step 5 In the System Event log, look at the Date and Time columns to find the first event in the current startup attempt.

Step 6 When you find the first event in this startup attempt, look for the first error that occurred after it. If no errors appear in the System Event log, contact Cisco TAC.

Step 7 Look at the value in the Source column for the first error and for any subsequent errors in the startup attempt.

If the value is Dlgc_log or DlgcDcm, the problem is with the installation or configuration of the Dialogic voice or fax cards. Double-click the event error to display additional information that may help you solve the problem. When a Dialogic service fails to start, you may need to check the IRQ settings, switches, jumpers, and rotary dials on each card, as applicable. When the Cisco Unity server contains more than one Dialogic voice card, you may also need to check the cable that connects the cards. Refer to the “Installing Voice Cards” section in the “Setting Up the Hardware” chapter of the *Cisco Unity Installation Guide* for additional information. The *Cisco Unity Installation Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst403/dom/index.htm.

If the Source column for an error has any other value, contact Cisco TAC.

Cisco Unity Administrator Browser Error Messages and Windows Error Messages

Cisco Unity administrators or subscribers may see the following error messages when they attempt to use the Cisco Unity Administrator or use Administrative Tools:

Error Message Access denied. Your class of service prohibits you from accessing the System Administration Web pages.

Explanation When this message appears during a logon attempt to the Cisco Unity Administrator, one of the following has occurred:

- The class of service for the logon account has been changed. Log on by using a different account.
- The Cisco Unity class of service has been changed to subscriber for everyone who previously had administrator privileges. There is no longer a Cisco Unity account for the administrator class of service.

Error Message Access denied. You cannot access the System Administration Web pages. Cisco Unity is not running.

Explanation When this message appears, Cisco Unity is not running. Cisco Unity must be running before anyone can log on to the Cisco Unity Administrator.

Recommended Action Start Cisco Unity.

Error Message Access denied. You cannot access the System Administration web pages. There are too many active sessions.

Explanation When this message appears, the maximum limit of concurrent system administration sessions has been reached.

Recommended Action Wait for an active session to be closed and then try again later.

Error Message Access denied. Your Windows Domain Account [Domain\login] is not associated with a Cisco Unity subscriber.

Explanation When this message appears during a logon attempt to the Cisco Unity Administrator, an invalid user name or password is being used.

Recommended Action Confirm the user name and password.

Error Message Additional users cannot be assigned to the class of service associated with the selected subscriber template. You have reached the license limit for one or more of the features enabled by the class of service.

Explanation Class of service can be used to restrict which licensed features are available to subscribers. If all available licenses for a feature are in use by a class of service, no new subscribers can be added to that class of service.

Recommended Action Go to the Subscribers > Class of Service > Features page for the class of service associated with the subscriber template. Determine if any of the licensed features used by that class of service are out of licenses, and if so, obtain sufficient additional licenses to meet subscriber needs. As a temporary measure until additional licenses are available, you can change the class of service associated with the selected subscriber template.

Error Message Failed to perform fetch against AvXml.dll. Check AvXml virtual directory settings in IIS for proper permissions and execute access. See the Troubleshooting Guide for details.

Explanation This error may appear when accessing the Status Monitor page.

Recommended Action Do the procedure [To Set Up Access to the Status Monitor After an Upgrade, page 10-4](#).

Error Message This page cannot be displayed. HTTP 403.1 Forbidden execute access forbidden.

Explanation This error may appear when Status Monitor access is attempted for the first time after an upgrade.

Recommended Action Do the following procedure.

To Set Up Access to the Status Monitor After an Upgrade

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

- Step 2** Click the **Default Web Site** directory, then locate the **Status** directory.
 - Step 3** Right-click the **Status** directory and browse to **Properties**.
 - Step 4** Click the **Virtual Directory** tab.
 - Step 5** Set Execute Permissions to **Scripts Only**.
 - Step 6** Click **OK**.
-

E-Mail and Voice Error Messages

Cisco Unity administrators can use the Event Monitoring System (EMS) to send e-mail and/or voice messages to other subscribers or distribution lists when an event occurs. Cisco Unity administrators or subscribers may see the following messages:

Error Message A conversation error has occurred.

Explanation A conversation error has occurred, sending a caller to the fail safe conversation.

Recommended Action Refer to the Windows Application Event log for more information about the error. If you are unable to determine the source of the problem from the information in the Application Event log, contact Cisco TAC.

Error Message Account locked—logon attempt limit reached.

Explanation An account is locked because the limit of unsuccessful phone logon attempts was reached.

Recommended Action Go to the Subscribers > Subscribers > Account page for the subscriber, and uncheck the Cisco Unity Account Status box to unlock the account. You can also refer to the Windows Application Event log for more information about the error.

Error Message All Ports Busy notification.

Explanation The voice server detected that all ports that are set to answer calls are busy. In this circumstance, incoming calls receive a busy signal and subscribers are unable to access the Cisco Unity conversation.

Recommended Action .In Cisco Unity Tools Depot, in the left pane under Reporting Tools, double-click Port Usage Analyzer. Run the Port Availability report. You may also find the Port Time Use report helpful. If the percentage of ports used exceeds 70 percent usage during peak periods, determine if additional answer ports are required, or if other adjustments to the port settings are needed. For more information, refer to the “Voice Messaging Port Settings” section in the “System Settings” chapter of the *Cisco Unity System Administration Guide*. The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.

Error Message Possible phone system integration failure.

Explanation The Cisco Unity server received an inbound call with no phone system integration information.

Recommended Action Refer to the Windows Application Event log for more information. If you are unable to determine the source of the problem from the information in the Application Event log, contact Cisco TAC.

Error Message System event notification.

Explanation Notification of a system event was attempted, but the notification text or voice message is missing or corrupt.

Recommended Action Refer to the Windows Application Event log for more information. If you are unable to determine the source of the problem from the information in the Application Event log, contact Cisco TAC.

Error Message That e-mail cannot be played at this time.

Explanation All of the licensed Text to Speech resources are in use.

Recommended Action Subscribers can try again later, or you may need to add more licenses.

Error Message Voice server hard disk almost full.

Explanation The Cisco Unity server hard disk is almost full. System logging and report data generation are terminated to conserve space.

Recommended Action Reclaim space on the hard disk to avoid potential loss of new messages and to resume logging and report generation. The Example Administrator account, which Cisco Unity creates during installation, serves as a default message recipient for the Unaddressed Messages and System Event Messages distribution lists. If you have not assigned another subscriber to these distribution lists, be sure to monitor the Example Administrator account and forward or delete the messages sent to this account as applicable. For subscribers on the Unaddressed Messages public distribution list, create a separate Inbox folder for returned messages. Then create a rule that automatically moves messages sent by the Cisco Unity Messaging System account from the Inbox to the returned messages folder.



Caution

Do not delete the Example Administrator unless you have assigned another subscriber to the Unaddressed Messages and System Event Messages distribution lists. Following Cisco Unity installation, the only member of these distribution lists by default is the Example Administrator. If these distribution lists contain no members, messages sent to them will be lost.

Error Message Voice server restart.

Explanation The Cisco Unity server stopped responding and was restarted.

Recommended Action Refer to the Windows Application Event log for more information about the error. If you are unable to determine the source of the problem from the information in the Application Event log, contact Cisco TAC.



Third-Party Fax Integration

About Problems With a Third-Party Fax Integration

Problems and troubleshooting procedures specific to a fax integration are described in this section.

A Subscriber Cannot Send or Receive Faxes

To Verify the Subscriber Fax Settings

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page for the subscriber.
 - Step 2** Click **View**.
 - Step 3** Confirm that the features for the class of service include FaxMail. For subscribers to have phone access to their faxes, they must be in a class of service (COS) that has the FaxMail feature selected. In addition, those subscribers who will have their e-mail messages delivered to a fax machine must be in a COS that has the Text to Speech feature selected.
 - Step 4** Confirm that the subscriber is listed as a fax user in the fax server database.
 - Step 5** If the subscriber is in a class of service with access to FaxMail, and is listed as a fax user in the fax server database, but still is unable to send or receive faxes, continue with the procedure in the [“A Subscriber Did Not Receive an Attached File Delivered to a Fax Machine”](#) section on page 11-1.
-

A Subscriber Did Not Receive an Attached File Delivered to a Fax Machine

Cisco Unity subscribers can have their e-mail messages delivered to a fax machine; however, if there are attachments to an e-mail message, Cisco Unity renders only those attachments with the file extensions specified during setup. Other types of attachments are removed, and Cisco Unity lists the file names at the end of the fax message. The fax domain name must also be correctly identified in Cisco Unity.

To view and Update Fax Domain Name and File Name Extensions

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

- Step 2** In the left pane of the Tools Depot window, under Administrative Tools, double-click **Third Party Fax Administration**.
- Step 3** Confirm the fax domain name and file extensions.
- Step 4** Click **Apply**.
- Step 5** Restart the Cisco Unity server.
-

A Fax Did Not Arrive at the Destination

If a subscriber records an introduction or adds any attachments to the body of a forwarded fax message, the Lotus Domino server resets the message type to e-mail. This causes Cisco Unity to be unable to recognize it as a fax, and the message is treated as an e-mail. Therefore, the message will not be reported in the fax message count, the fax message notification will not work, and the fax phone conversation will not present the option to forward the message to a fax machine.

To Research a Missing Fax

- Step 1** Look for any forwarded fax messages with attachments and/or with a voice introduction by using the Lotus Notes client. The missing fax message will most likely appear as an e-mail message. If the fax message is not present, continue with [Step 2](#).
- Step 2** Verify the fax phone number. Ask the subscriber to resend the fax to confirm that the problem was not with the receiving station or with an incorrect fax phone number.
- Step 3** In the fax server administration program, look for the fax in the outbound queue.
If the fax is there, continue with [Step 4](#).
If the fax is not there, verify the configuration of the fax gateway, make changes as necessary, and resend the fax. If the fax still is not in the queue, contact Cisco TAC.
- Step 4** Confirm that the fax server is configured correctly for the fax card(s) that are installed.
If the server is not configured correctly, make changes as necessary and resend the fax.
If the server is configured correctly, the problem is most likely with the fax card(s). Contact Cisco TAC.
-

Related Documentation

- The “Overview: Fax Server Integration” section in the “Integrating a Fax Server with Cisco Unity” chapter of the *Cisco Unity System Administration Guide*. The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.



Utilities

Tools Depot

Tools Depot allows access to most Cisco Unity tools from a single location. The Cisco Unity Tools Depot icon is available on the Cisco Unity server desktop.

The left pane of the Tools Depot window lists all available tools by category. To display online Help for a tool, click the name in the left pane. To run the tool, double-click the name.

Some tools work only with selected versions of Cisco Unity. If a tool does not appear in the Tools Depot, it does not work with the version of Cisco Unity currently running.

For more information on Cisco Unity tools, see the following sections:

Integration Monitor	Shows the information being sent between the phone system and Cisco Unity. See the “Integration Monitor” section on page 12-1.
Learn Tones	Learns the frequency and cadence of the phone system tones and updates the phone system template file. See the “Learn Tones” section on page 12-5.
Call Viewer	Displays information about each call that the phone system integration sends to Cisco Unity. See the “Call Viewer” section on page 12-10.
Cisco Unity Diagnostic Tool	Contains a database of possible Cisco Unity problems and controls the gathering of diagnostic traces used to troubleshoot these problems. See the “Cisco Unity Diagnostic Tool” section on page 12-11.
Advanced Settings Tool	Allows updating of hidden registry settings and addition of new registry keys. See the “Advanced Settings Tool” section on page 12-13.
Universal Dialogic Diagnostics utility	Performs a wide range of tests on the Dialogic voice cards. See the “Universal Dialogic Diagnostics Utility” section on page 12-14.
Port Status Monitor	Can be used to monitor call activity. See the “Port Status Monitor” section on page 12-15.

Integration Monitor

The Integration Monitor shows the information being sent between the phone system and Cisco Unity. Each packet of data contains information on one call that the phone system forwards to Cisco Unity. In some cases, seeing this data can help you diagnose integration problems.

With a serial integration, you can view the packets of data that are sent over the serial link. The Integration Monitor also displays the packets that Cisco Unity sends to the phone system, each of which contains one MWI on or off code.

With an DTMF (analog) integration, you can view the packets sent over the analog phone lines that connect the phone system and Cisco Unity.

When troubleshooting IP integrations (such as Cisco CallManager or SIP), use the Call Viewer. The Cisco Unity Integration Monitor is not compatible with IP integrations. See the “[Call Viewer](#)” section on page 12-10 for more information.

To Run the Integration Monitor

-
- Step 1** Cisco Unity must be running for the Integration Monitor to display the packets being passed to and from the Cisco Unity server. If Cisco Unity is not running, start it.
 - Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 3** In the left pane of the Tools Depot window, in the Switch Integration Tools directory, double-click **Integration Monitor**.
 - Step 4** Use the **View** menu to select display options. For more information, see the “[Integration Monitor Display Options](#)” section on page 12-3.
-

Values Displayed in the Integration Monitor

For information on the values and menu options that appear in the Integration Monitor, see [Table 12-1](#).

Table 12-1 Integration Monitor Fields and Columns

Field/Column	Meaning
Analog Integration or Serial Integration	Immediately below the menu bar, the Integration Monitor displays the name of the current integration and the integration type.
First Digit Delay (ms) <i>(DTMF or analog integrations only)</i>	The amount of time that Cisco Unity waits (in milliseconds) for the first digit of a packet to arrive after Cisco Unity answers a call. For example, to specify that the Integration Monitor wait three seconds for the first digit to arrive, enter 3000. If you change this value, you are changing the value in the Cisco Unity phone system template file for the current integration. Changing this value may cause Cisco Unity to work incorrectly.
Next Digit Delay (ms) <i>(DTMF or analog integrations only)</i>	The amount of time that Cisco Unity waits between digits for the next digit of a packet to arrive. If the next digit does not arrive within that amount of time, Cisco Unity considers the next digit user input, and the Integration Monitor displays the digit on a new line (only when the Include digits option and Hang-up packet are defined). For example, to specify that the Integration Monitor wait two-tenths of a second for the next digit to arrive, enter 200. If you change this value, you are changing the value in the Cisco Unity phone system template file for the current integration. Changing this value may cause Cisco Unity to work incorrectly.
Time	The time at which Cisco Unity received the call from the phone system or the time at which Cisco Unity sent an MWI on or off code to the phone system. New packets appear at the top of the Integration Events list.

Table 12-1 Integration Monitor Fields and Columns (continued)

Field/Column	Meaning
Packet	The unformatted information that the phone system sent to Cisco Unity or that Cisco Unity sent to the phone system. The Integration Monitor uses the phone system template file to parse the contents of the packet into the values in the remaining columns.
Port	The voice card port on the Cisco Unity server on which a call arrives from the phone system.

Integration Monitor Display Options

The menus in the Integration Monitor allow you to save data to a file and change the display in a variety of ways, as described in [Table 12-2](#).

Table 12-2 Integration Monitor Options

Menu	Option	Description
File	Log to file	To specify a file for saving Integration Monitor data.
Edit	Allow delay edits <i>(DTMF or analog integrations only)</i>	To change the values in the First Digit Delay (ms) and Next Digit Delay (ms) fields. If this option is not selected, the values are display only. For more information, see First Digit Delay (ms) and Next Digit Delay (ms) in Table 12-1 .
View	Always on top	To display the Integration Monitor window in front of all other windows regardless of which window is currently active. To cancel the option, click it again.
View	Include digits <i>(DTMF or analog integrations only)</i>	To display individual digits that are not recognized as part of a packet. For more information, see Next Digit Delay (ms) in Table 12-1 .
View	Freeze display	To prevent new data packets from being displayed in the Integration Monitor window. If Cisco Unity is busy, this option can be useful for analyzing an individual packet. Freezing the display prevents the packet from scrolling out of the window before you can look at it. To unfreeze the display, click the option again.
View	Raw serial data <i>(serial integrations only)</i>	To display data from the phone system or from Cisco Unity regardless of whether the Integration Monitor recognizes the data as a valid packet. If no data is displayed in the Integration Monitor but you think it should be, try this option. There may be no display because the Integration Monitor is unable to determine what the pieces of the packets are. To return to displaying formatted packets, click the option again.
View	Outgoing data <i>(serial integrations only)</i>	To display only the packets that Cisco Unity is sending to the phone system to turn MWIs on and off. To return to displaying all packets, click the option again.

Table 12-2 Integration Monitor Options (continued)

Menu	Option	Description
View	Incoming data only (serial integrations only)	To display only the packets that the phone system is sending to Cisco Unity, including: <ul style="list-style-type: none"> • Calls forwarded to Cisco Unity because the extension is busy. • Calls forwarded to Cisco Unity because the extension is not answered. • Calls forwarded to Cisco Unity because the extension is in do not disturb mode. • Calls from subscribers who want to check or leave voice messages. • Calls from external callers who called Cisco Unity. To return to displaying all packets, click the option again.

Frequently Asked Questions About the Integration Monitor

Question	Answer
Can I freeze the display?	Yes. On the View menu, click Freeze Display.
Can I view raw serial data?	Yes. On the View menu, click Raw Serial Data.
Can I view DTMF digits (analog only) separately from the packets?	Yes. On the View menu, click Include Digits, and confirm that the Hang-up packet is defined. This view lets you see all packets and all other DTMF digits detected by Cisco Unity and can be helpful in troubleshooting DTMF integration packet problems.
Can I log the integration packets in the Integration Monitor to a file?	Yes. On the File menu, click Log to File. Specify name and location of the file to receive the integration packet information.
Can the Integration Monitor be used with all integrations?	No. The Integration Monitor can be used only for serial and DTMF (analog) integrations. For IP integrations (such as Cisco CallManager and SIP), use the Call Viewer. See the “Call Viewer” section on page 12-10 for more information.

Integration Monitor Troubleshooting

To Resolve a Situation Where No Integration Information Is Displayed for a Serial or DTMF Integration

- Step 1** In the View menu, confirm that Freeze Display is not selected. If it is selected, deselect it.
- Step 2** On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
- Step 3** Confirm that the settings match those indicated in the integration guide for your phone system.
- Step 4** Correct any incorrect values.
- Step 5** If you changed values in [Step 4](#), click **Save**, and continue with [Step 6](#). If you did not change any values, skip to [Step 7](#).
- Step 6** If prompted, restart the Cisco Unity server.

- Step 7** If you have a serial integration, confirm that the serial cable is plugged securely into the correct Cisco Unity COM port and into the phone system serial port.
- If none of the steps in this procedure correct the problem, contact the Cisco Technical Assistance Center (TAC).
-

To Resolve a Situation Where Only Partial Packets Appear (DTMF or Analog Integrations Only)

- Step 1** On the Integration Monitor Edit menu, click **Allow Delay Edits**.
- Step 2** Increase the values in the First Digit Delay (ms) and Next Digit Delay (ms) fields. For example, if the First Digit Delay (ms) field is set to 2000, change it to **3000**. And if the Next Digit Delay (ms) field is set to 250, change it to **500**.
- Step 3** On the Integration Monitor Edit menu, click **Allow Delay Edits** again to save the changes.
- Step 4** If partial packets still appear, contact Cisco TAC for assistance in changing the OffHook delay parameter.
-

Learn Tones

Cisco Unity comes with template files for a variety of phone systems. These template files usually work without modification. However, problems with transfers, message waiting indicators (MWIs), and message notification can arise if Cisco Unity does not understand the phone system tones. If any of these problems occur, and basic troubleshooting procedures do not correct the problem, run the Learn Tones utility to modify the phone system template file.

The Learn Tones utility is designed to run on systems equipped with Dialogic analog voice cards only. The Learn Tones utility also requires exclusive access to the ports. Do not run Learn Tones unless Cisco Unity is shut down.

The Learn Tones utility learns the frequency and cadence of the phone system tones, such as busy and ringback, and teaches them to Cisco Unity. Once you start the utility, the process is automatic. One voice messaging port calls other ports to generate the tones. The utility displays the tone settings already present in the phone system template file on start-up, and sets any missing items to the default values. Upon completion, it adds the learned tones of your choice to the phone system template file.

Tones Defined in the Switch Configuration File

There are five different tones that can be defined in the Cisco Unity switch configuration file. These can be split into two categories. The first category is tones that are used during call progress. Cisco Unity listens for these tones when performing a transfer or making an outgoing call, but does not listen for these tones during the voice mail conversation or during recording. These tones are:

- Switch Dial Tone
- Switch Ringback Tone
- Switch Busy Tone

The other two tones are disconnect tones. Cisco Unity always listens for these tones during voice messaging conversation and during recording. If one of these tones is detected, it tells Cisco Unity that the caller has hung up, and Cisco Unity goes on hook. These tones are:

- Switch Disconnect Tone
- CO Disconnect Tone

There are usually no tone definitions in the switch configuration file when the Cisco Unity system is installed. Depending on the phone system and integration being used, it is often unnecessary to define any tones in the switch configuration file. Cisco Unity uses a default set of definitions for tones that are not defined in the switch configuration file, and this default set usually works. When it is determined that a particular tone (or tones) must be defined in the switch configuration file, it is best to define only that tone. Defining tones that are not necessary for Cisco Unity to perform properly with a particular phone system can limit the ability of the voice messaging system to handle unexpected tones, such as unexpected disconnect tones sent from a PSTN.

Learning tones may resolve the problem when callers report being disconnected (hung up on) while they are recording a voice message. The default disconnect tone definitions in Cisco Unity have very large frequency and cadence deviations defined. While this allows the system to detect disconnect tones from a wide range of central offices, phone systems, countries, and so on, it also increases the chance that the voice of a caller will mistakenly be detected as disconnect tone, causing the voice messaging system to hang up on the call. Learning the disconnect tones specific to the phone system in use can remedy this problem. Once the tone definition is in the switch configuration file, the deviations can be manually edited if fine tuning is desired.

Switch Configuration File Location

The switch configuration.ini files are located in the \CommServer\Intlib directory on the Cisco Unity server. The active switch configuration file is based on the selections made in the UTIM during Cisco Unity installation, or by any subsequent changes made in the Edit Switch utility.

Running the Learn Tones Utility

Do the following procedure to run the Learn Tones utility.

To Run the Learn Tones Utility (on Systems Equipped with Dialogic Analog Cards Only)

-
- Step 1** Shut down the Cisco Unity software.
 - Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 3** In the left pane of the Tools Depot window, in the Switch Integration Tools directory, double-click **Learn Tones**.
 - Step 4** Confirm that all ports and extensions are correct. Do not use a hunt group for the helper extension.
 - Step 5** Choose Manual mode or allow Learn Tones to run in Automatic (default) mode.

Both modes use port 1 as the primary learning port, and Automatic mode uses ports 2 and 3 as helper ports. Or, you can designate other helper ports by entering their port numbers and extensions. Extension numbers for ports 1, 2, and 3 are imported automatically from the Cisco Unity Administrator Ports page.

Use Manual mode when you want the primary port to call a specific extension rather than a helper port, or when some aspect of the phone system programming, such as forwarding when a line is busy, conflicts with the tone-learning process. The phone specified for Manual mode should be close to the Cisco Unity

server, so that you can see the on-screen prompts and operate the phone at the same time. To run in Manual mode, check the **Manual Mode** check box under Settings, and enter the extension of the phone you want to use in the Manual Ext field.

- Step 6** Confirm that the Delay Between Calls field is set to the default value of **4000 ms**. Delay between calls is the number of milliseconds that Learn Tones delays before making a subsequent call to learn or verify a tone.
- Step 7** Confirm that the Deviation Threshold field is set to the default value of **15 percent**. The Deviation Threshold field sets the deviation that is considered acceptable when learning individual tones. Tones outside the Deviation Threshold field setting for any single field (frequency 1, frequency 2, on, off, and so on) are discarded.
- Step 8** Confirm that the Calls field is set to the default value of **1**.
- Step 9** Confirm that the Frames field is set to the default value of **5**.
- Step 10** Confirm that the Delay(ms) field is set to the default value of **1500 ms**. The Delay field sets the amount of time between the completion of the action to cause a tone, and the beginning of learning the tone. The delay value avoids detection of stray events on the line during line state transitions.
- Step 11** To learn dial tone, in the Dialtone section, click **Learn**. In Automatic mode, Learn Tones uses the following process to learn dial tone:
- Goes off-hook on port 1.
 - Waits the number of milliseconds defined in the Delay field for dial tone.
 - Listens to and learns the tone on port 1.
 - Goes on-hook on port 1.
 - Waits the number of milliseconds defined in the Delay Between Calls field.
 - Listens to and verifies the tone on port 1.
 - Goes on-hook on port 1.

If a “Success” message appears at the conclusion of this process, continue with [Step 12](#).

If a “Failure” message appears, resolve the problem and repeat this step.

- Step 12** To learn busy tones, in the Busy section, click **Learn**. In Automatic mode, Learn Tones uses the following process to learn busy tone:
- Goes off-hook on port 2.
 - Dials port 3 extension.
 - Goes off-hook on port 3 to answer the call from port 2.
 - Goes off-hook on port 1.
 - Dials port 2 extension.
 - Waits the number of milliseconds defined in the Delay field for busy tone.
 - Listens to and learns the tone on port 1.
 - Goes on-hook on ports 1, 2, and 3.
 - Waits the number of milliseconds defined in the Delay Between Calls field.
 - Goes off-hook on port 2.
 - Dials port 3 extension.
 - Goes off-hook on port 3 to answer the call from port 2.
 - Goes off-hook on port 1.

- n. Dials the extension of port 2.
- o. Listens to and verifies the tone on port 1.
- p. Goes on-hook on ports 1,2 and 3.

If a “Success” message appears at the conclusion of this process, continue with [Step 13](#).

If a “Failure” message appears, resolve the problem and repeat this step.

Step 13 To learn the phone system disconnect tone, in the Disconnect section, click **Learn**. In Automatic mode, Learn Tones uses the following process to learn disconnect tone:

- a. Waits the amount of milliseconds defined in the Delay Between Calls field.
- b. Goes off-hook on port 1.
- c. Dials port 2 extension.
- d. Goes off-hook on port 2 to answer the call from port 1.
- e. Delays for 2000 ms (2 seconds).
- f. Goes on-hook on port 2.
- g. Waits the amount of milliseconds defined in the Delay field for disconnect tone.
- h. Listens to and learns the tone on port 1.
- i. Goes on-hook on port 1.
- j. Waits the amount of milliseconds defined in the Delay Between Calls field.
- k. Goes off-hook on port 1.
- l. Dials port 2 extension.
- m. Goes off-hook on port 2 to answer the call from port 1.
- n. Delays for 2000 ms (2 seconds).
- o. Goes on-hook on port 2.
- p. Listens to and verifies the tone on port 1.
- q. Goes on-hook on port 1.

If a “Success” message appears at the conclusion of this process, continue with [Step 14](#).

If a “Failure” message appears, resolve the problem and repeat this step.

Step 14 To learn CO Disconnect tone, in the CO Disconnect section, click **Learn**. In Automatic mode, Learn Tones uses the following process to learn CO disconnect tone:

- a. Goes off hook on port 1.
- b. Dials 9.
- c. Waits the amount of milliseconds defined in the Delay field for CO Disconnect tone.
- d. Listens to and learns the tone on port 1.
- e. Goes on-hook on port 1.
- f. Waits the amount of milliseconds defined in the Delay Between Calls field.
- g. Goes off-hook on port 1.
- h. Dials 9.
- i. Listens to and verifies the tone on port 1.
- j. Goes on hook on port 1.

If a “Success” message appears at the conclusion of this process, continue with [Step 15](#).

If a “Failure” message appears, resolve the problem and repeat this step.

Step 15 To learn ringback tone, in the Ringback section, click **Learn**. In Automatic mode, Learn Tones uses the following process to learn ringback tone:

- a. Goes off-hook on port 1.
- b. Dials the extension of port 2.
- c. Waits the amount of milliseconds defined in the Delay field for ringback tone.
- d. Listens to and learns the tone on port 1.
- e. Goes on hook on port 1.
- f. Waits the amount of milliseconds defined in the Delay Between Calls field.
- g. Goes off-hook on port 1.
- h. Dials the extension of port 2.
- i. Listens to and verifies the tone on port 1.
- j. Goes on hook on port 1.

If a “Success” message appears at the conclusion of this process, continue with [Step 16](#).

If a “Failure” message appears, resolve the problem and repeat this step.

Step 16 The Learn Tones utility automatically verifies tones after it learns them, so there is no need to click Verify All before saving the learned tones.

Step 17 Click **Save**.

Step 18 In the dialog box that appears, check only the check boxes of the tones you want to update in the switch configuration file, then click **OK**.

Step 19 To save the new tones directly to the active switch configuration file, accept the default file name. If you want to save the tones to a temporary file for comparison and then manually copy them to the switch configuration file at a later time, enter a file name of your choice. Click **Open**.

Step 20 Click **Done** to exit the Learn Tones utility.

Step 21 Restart the Cisco Unity software.

Troubleshooting the Learn Tones Utility

If the learn tones process fails, do one or more of the following:

- Adjust the setting in the Delay field for the tone that you are having trouble with. 1500 to 2000 milliseconds is usually sufficient. Be careful not to make this delay too long as Learn Tones may fail to learn a tone, learn the wrong tone, or miss the tone altogether.
- If Automatic mode is not working, try Manual mode, or vice versa.
- Unplug the line cord from port 1 of Cisco Unity and plug it into an analog phone. Use the same steps that the Learn Tones utility uses to manually recreate the condition that Learn Tones is listening to.

- If one or more tones are learned with the cadence shown in the following table,

On(ms)	Dev	Off(ms)	Dev
2000	-2000	0	0

the learned tone is continuous. When a tone with continuous cadence is saved to the switch configuration file, the cadence appears as:

```
TimeOn1=4000
TimeOnDeviation1=0
TimeOff1=0
TimeOffDeviation1=0
Cycles=0
```

This is intentional. To support voice card manufacturers other than Dialogic, the latter method must be used when defining a continuous tone in the switch configuration file. When Cisco Unity is restarted, the Miu translates the cadence back to the original settings if Dialogic cards are installed.

- If you need assistance resolving these or other Learn Tones problems, contact Cisco TAC.

Call Viewer

For each call that the phone system integration sends to Cisco Unity, 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.

The Call Viewer displays integration information for inbound calls only. To see call information for outbound calls, use the StatusMonitor, located in the Tech Tools directory.

Note that if you are troubleshooting a Cisco CallManager integration, you must use the Call Viewer; the Cisco Unity Integration Monitor is not compatible with a Cisco CallManager integration.

To Run the Call Viewer

-
- Step 1** If Cisco Unity is not running, start it.
 - Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 3** In the left pane of the Tools Depot window, in the Switch Integration Tools directory, double-click **Call Viewer**.
 - Step 4** Use the Call Viewer window to see call information that the phone system integration provides to Cisco Unity for inbound calls.
-

Cisco Unity Diagnostic Tool

The Cisco Unity Diagnostic Tool allows creating and viewing of diagnostic log files that can be used to troubleshoot problems. It replaces the diagnostic log functionality in Maestro Tools, and allows the system administrator or TAC staff to selectively run diagnostic traces at two levels:

- **Macro Traces**—These are collections of component traces that help diagnose problems such as message waiting indicator and system problems.
- **Micro Traces**—These are the component traces. Each component has up to 32 trace levels that can be individually selected.

The Cisco Unity Diagnostic Tool also allows the system administrator or TAC staff to do the following tasks:

- **Create new log files on demand.** This makes troubleshooting problems easier. When a problem can be reproduced reliably, the system administrator can close all existing log files and create new log files prior to reproducing the problem. This eliminates many unnecessary and unrelated items from the logs.
- **Configure log settings.** The system administrator can adjust the maximum disk space allowed for all diagnostic log files. (The default setting is 400 MB.) The Logging Properties screen also allows the system administrator to disable all diagnostic output by clearing the Diagnostic Output check box.
- **Gather standard logs.** This option provides the ability to quickly gather all or selected Microsoft Windows and Cisco Unity logs.
- **Disable all traces.** This is a quick way to return diagnostic logs to their default settings after troubleshooting efforts are complete.
- **View the Event log.** The Event log files for either the local computer or another computer can be viewed and exported.
- **Change the display language for Windows Event log messages that are generated by Cisco Unity.** This is a temporary change and is only in effect while the Cisco Unity Diagnostic Tool is running.

To View and Export Diagnostic Files by Using the Cisco Unity Diagnostic Tool

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **Unity Diagnostic Tool**.
 - Step 3** On the left pane of the Cisco Unity Diagnostic Viewer screen, click **Processes**. The node expands to list each process that uses log manager.
 - Step 4** Click a process node and then click a log file. The selected log file is formatted and displayed in the right pane.
 - Step 5** To export or save a copy of the log file, click **Action > Export List**.
 - Step 6** Name the file and save it to a location of your choice in .txt or .csv format.
-

To Create Macro or Micro Diagnostic Traces for Troubleshooting

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

- Step 2** In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **Unity Diagnostic Tool**.
 - Step 3** On the Cisco Unity Diagnostic Viewer screen, click either the **Configure Macro Traces** icon, or the **Configure Micro Traces** icon, as applicable.
 - Step 4** Follow the on-screen instructions.
 - Step 5** On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.
 - Step 6** Reproduce the problem.
 - Step 7** View and export the results by doing the procedure [To View and Export Diagnostic Files by Using the Cisco Unity Diagnostic Tool, page 12-11](#).
 - Step 8** On the Cisco Unity Diagnostic Viewer screen, click the **Disable All Traces** icon to turn off the traces set in [Step 3](#).
 - Step 9** In the Disable All Traces Wizard screen, check the **Disable All Traces** check box, and click **Finish**.
-

To Access the Event Viewer on Another Computer

- Step 1** In the left pane of the Cisco Unity Diagnostic Tool window, right-click **Event Viewer (Local)**.
 - Step 2** Click **Connect to Another Computer**.
 - Step 3** Browse to select a computer on the list.
 - Step 4** Click **OK**.
 - Step 5** Select and view the log file.
 - Step 6** To export or save a copy of the log file, click **Action > Export List**.
 - Step 7** Name the file and save it to a location of your choice in .txt or .csv format.
-

To Change the Windows Event Log Display Language for Cisco Unity-Generated Messages

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **Unity Diagnostic Tool**.
- Step 3** In the left pane of the Cisco Unity Diagnostic Tool, click **Cisco Unity Diagnostic Tool > Processes**. The node expands to list each process that uses log manager.
- Step 4** Right-click **Processes** or the individual process node of your choice.
- Step 5** Click **Change Cisco Unity Event Log Language**.
- Step 6** Click a new language from the list of available languages.
- Step 7** Click **Apply**, then click **OK**.
- Step 8** In the left pane of the Cisco Unity Diagnostic Tool, click **Event Viewer (Local)**, and then click the log file category you wish to view.



Note When the Cisco Unity Diagnostic Tool is closed, Cisco Unity Event log messages revert to the original language.

Advanced Settings Tool

The Advanced Settings Tool allows system administrators to safely edit many of the Cisco Unity hidden registry settings. It gives a brief overview of each setting, limits edits to specific value ranges, and ensures that edits are consistent with the installed Cisco Unity version.

To Edit an Existing Registry Key

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click the key name.
- Step 4** In the **New Value** box or list, click or enter the applicable value, then click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.
- Step 7** If applicable, restart the Cisco Unity server for the registry change to take effect.

To Add a New Registry Key

Adding a new registry key to the database should be done only when indicated in the Cisco Unity documentation, or on the advice of Cisco TAC. Note that the add function can also be used to display information about existing registry settings.

- Step 1** Open a command prompt window, and browse to the CommServer\Utilities\Advanced Settings Tool directory.
- Step 2** Enter **start unityadvancedsettingstool /addkey** and press **Enter**. The Unity Advanced Settings page appears.
- Step 3** On the Unity Advanced Settings page, click **Add New Key**.
- Step 4** On the Add New Registry Key page, click **Add New**. Enter information in the following fields as applicable.

Field Name	Description
Index	<i>Display only.</i> A read-only field that displays a unique number for each record in the database.
Short Description	Enter a description of the registry key change (maximum of 250 characters).
Long Description	Enter a description of the behavior change that the registry key invokes.

Field Name	Description
Key Path	Enter the path to the directory where the key is stored. All values are assumed to be under HKEY_LOCAL_MACHINE. If you need to set values outside of this registry branch, do not use this tool. Use Regedit instead.
Key Name	Enter the name of the registry at the key path. In the rare case of a registry setting that is only the key path and not a key value, you can leave this field blank.
Key Type	Select a value on the list, as follows: <ul style="list-style-type: none"> • REG_SZ—string values. • REG_DWORD—number values. • REG_BINARY—binary values (not used). • NONE—for cases where the presence of the key path is all that is needed, rather than a key with a value. This value should be used rarely, if at all.
Minimum Value	Enter the minimum allowable value, if the key type is a number. String values do not use this field.
Maximum Value	Enter the maximum allowable value, if the key type is a number. String values do not use this field.
Step By	Enter the step for each value added to the drop-down list, if the key type is a number. For example, if the minimum value is 0, and the maximum value is 100, a Step By value of 20 will populate the drop-down list with 0, 20, 40, 60, 80, 100.
Minimum Unity Version	A list of all Cisco Unity versions 2.3 and later. Indicate if the registry key is not valid for versions earlier than a specified version.
Maximum Unity Version	A list of all Cisco Unity versions 2.3 and later. Indicate if the registry key is not valid for versions later than a specified version.

Step 5 Click **Save**, and then click **OK**.

Step 6 Click **Exit**.

Universal Dialogic Diagnostics Utility

The Universal Dialogic Diagnostics (UDD) utility performs a wide range of tests on the Dialogic voice cards. It is used to determine if something is wrong with one or more of the Dialogic voice cards in the Cisco Unity server.

To Run the UDD Utility

Step 1 On the Windows Start menu, click **Programs > Dialogic System Software > Universal Dialogic Diagnostics Utility**.

Step 2 On the Service menu, click **Stop Service**.

- Step 3** The UDD utility may display several warning or error messages. For each, choose the option that continues the process of starting the utility.
 - Step 4** Select the options required to do all tests on all voice cards. The tests take approximately five minutes per voice card.
 - Step 5** When the tests are finished, the Done button becomes available. Click **Done** to display additional information on failed tests, if any.
 - Step 6** If you see errors that you do not know how to resolve, contact Cisco TAC.
 - Step 7** When you are finished reviewing test results, click **Exit UDD**.
 - Step 8** Shut down and restart the Cisco Unity server.
-

Port Status Monitor

Cisco Unity has two Status Monitors: the web-based Status Monitor that is described in the *Cisco Unity System Administration Guide*, and the Port Status Monitor that is located in the Switch Integration Tools directory of Tools Depot.

Both are useful as troubleshooting tools. However, the web-based Status Monitor is not intended to be run for long periods of time due to the significant amount of system resources it utilizes. The web-based Status Monitor automatically times out after 20 minutes of use while the Port Status Monitor application does not adversely impact system performance and can be run for as long as necessary to monitor call activity and troubleshoot a problem.



Subscriber and Administrator Access

About Access Problems

Subscriber access problems are usually related to a problem with the phone system integration. Subscriber access problems may include:

Problems that prevent subscribers from using Cisco Unity	See the following sections, as applicable: <ul style="list-style-type: none">• Subscribers Logging On to Cisco Unity Hear the Opening Greeting Instead of the Subscriber Conversation, page 13-2.• Cisco Unity Does Not Respond to Touchtones, page 13-2.
Problems that prevent subscribers from fully utilizing the features of Cisco Unity and the phone system	See the following sections, as applicable: <ul style="list-style-type: none">• Cisco Personal Communications Assistant Pages Cannot Be Opened or Have Been Defaced, page 13-4.• Subscribers Cannot Access Cisco Personal Communications Assistant Pages, page 13-5.• Subscribers Cannot Access the Cisco Unity Assistant from the Cisco PCA, page 13-6.• Subscribers Cannot Save Changes on Pages in the Cisco Unity Assistant, page 13-6.• No Sounds Play on the Multimedia System After Installing the Cisco CallManager Software, page 13-7.• Subscribers Cannot Be Located in a New or Updated Directory Handler, page 13-7.

Administrator access problems can include a missing tray icon, or missing or defaced web pages. See the [“Cisco Unity Tray Icon Is Missing from the Status Bar”](#) section on page 13-8, and the [“Cisco Unity Administrator or Status Monitor Pages Cannot Be Opened or Have Been Defaced”](#) section on page 13-8.

If you encounter a subscriber or administrator access problem that is not described in these sections, contact the Cisco Technical Assistance Center (TAC).

Subscribers Logging On to Cisco Unity Hear the Opening Greeting Instead of the Subscriber Conversation

Confirm that the integration is enabled and that the phone system settings are correct.

To Verify the Phone System Settings in the Cisco Unity Administrator

-
- Step 1** On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
 - Step 2** Confirm that the settings match those indicated in the integration guide for your phone system.
 - Step 3** Correct any incorrect values for the phone system.
 - Step 4** If you changed values in [Step 3](#), click **Save**.
 - Step 5** If prompted, restart the Cisco Unity server.
 - Step 6** If you have confirmed that the integration is enabled and that the phone system settings are correct, and subscribers still hear the opening greeting instead of the subscriber conversation, contact Cisco TAC.
-

Cisco Unity Does Not Respond to Touchtones

There are several possible reasons that Cisco Unity may not respond to touchtones. Use the [“Task List for Troubleshooting Problems with Touchtones”](#) to troubleshoot the possible causes.

Task List for Troubleshooting Problems with Touchtones

1. (Cisco CallManager only) Confirm that DTMF relay is enabled through VoIP dial-peer gateways. See the [“DTMF Signal Is Not Being Sent \(Cisco CallManager Only\)”](#) section on page 13-2.
2. (Circuit-switched phone systems only) Confirm that the DTMF signal is being sent. See the [“DTMF Signal Is Not Being Sent \(Circuit-Switched Phone Systems Only\)”](#) section on page 13-3.
3. (Circuit-switched phone systems only) Confirm that the DTMF values are consistent with Cisco Unity and the phone system. See the [“DTMF Values in Cisco Unity Are Inconsistent with the Values in the Phone System \(Circuit-Switched Phone Systems Only\)”](#) section on page 13-4.

DTMF Signal Is Not Being Sent (Cisco CallManager Only)

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 Cisco Unity, use the following command:
- ```
dtmf-relay h245-alphanumeric
```
- Step 2** Create a destination pattern that matches the Cisco 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 Cisco Unity.
- 

## DTMF Signal Is Not Being Sent (Circuit-Switched Phone Systems Only)

The first procedure in this section is used only for feature-set phones, because feature-set phones rely on the phone system to generate touchtones, while analog phones generate their own touchtones. For feature-set phones, you may need to enable touchtones on the phone system.

If you are having trouble only with the operator console, skip to the procedure [To Test Manual DTMF Signaling on the Operator Console, page 13-3](#).

If you are using only analog phones to access Cisco Unity and are having trouble with response to touchtones, contact Cisco TAC.

### To Test Manual DTMF Signaling on Feature-Set Phones

Do this procedure for each type of feature-set phone that you use to access Cisco Unity.

- 
- Step 1** Set up a test phone (Phone 1) for single-line testing. For more information, see the [“Preparations for Troubleshooting the Phone System” section on page 1-1](#).
- Step 2** On a feature-set phone that is connected to the phone system but that is not connected to Cisco Unity (Phone 2), call Phone 1. For Phone 2, use a phone that is the same type that subscribers use to access Cisco Unity.
- Step 3** Answer Phone 1.
- Step 4** On Phone 2, press touchtone keys.
- If you hear touchtones on Phone 1, the type of phone you are using for Phone 2 is sending DTMF signals to Cisco Unity. Continue with [Step 5](#).
- If you do not hear touchtones, reprogram the phone system to provide station-to-station DTMF signaling on that line, and repeat the test. If you still do not hear touchtones, contact the phone system vendor.
- Step 5** Connect a line-monitoring device (for example, a ZiadLinemaster) to Phone 1, and test the duration and volume of the touchtones Phone 2 is generating. Write down the values, and contact Cisco TAC to determine whether touchtone durations in the phone system template file need to be changed. For information on setting up the line-monitoring device, refer to the documentation from the manufacturer.
- 

### To Test Manual DTMF Signaling on the Operator Console

- 
- Step 1** Do the procedure [To Test Manual DTMF Signaling on Feature-Set Phones, page 13-3](#), but use the operator console for Phone 2.

- Step 2** If you hear touchtones on Phone 1, the operator console is sending DTMF signals to Cisco Unity. The reason Cisco Unity is not responding to touchtones is most likely related to the Cisco Unity setup. Contact Cisco TAC.
- If you cannot hear touchtones on Phone 1, the operator console is not generating touchtones. Add a tone dialer that generates DTMF tones, and repeat the test.
- If you still cannot hear touchtones, contact Cisco TAC.
- 

## DTMF Values in Cisco Unity Are Inconsistent with the Values in the Phone System (Circuit-Switched Phone Systems Only)

### To Compare Phone System and Cisco Unity Values for DTMF Duration and Delay Between Digits

---

- Step 1** In the phone system documentation or programming, locate the duration of DTMF tones and the delay between digits that the phone system expects from Cisco Unity.
- Step 2** On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Edit Switch Utility**. The Switch Configuration Editor window appears.



**Caution** Do not use the Edit Switch utility to change values without contacting Cisco TAC for assistance.

---

- Step 3** Confirm that the phone system Cisco Unity is integrated with appears in the fields, then click **Edit This Switch Configuration**.
- Step 4** In the Switch Configuration dialog box, click the **Outdial** tab.
- Step 5** Compare values in the Dialed DTMF Duration and Delay Between Dialed DTMF Digits fields with the the phone system values. If the values do not match, contact Cisco TAC.
- 

## Cisco Personal Communications Assistant Pages Cannot Be Opened or Have Been Defaced

If the Cisco Personal Communications Assistant (PCA) installation fails, or if someone inadvertently deletes some or all of the Cisco PCA files from the Cisco Unity server after installation, the Cisco PCA web pages may be defaced or become unusable. Virus incidents and attacks from hackers can cause the same problems.

If you have the Cisco Unity installation disks, you can restore corrupt or missing Cisco PCA files and applications by running an installation script at a command prompt. When you restore the Cisco PCA, the installation script removes any existing Cisco PCA-related files and applications, including the Tomcat service and its integration to the IIS server.



**Caution** Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

---

If the Cisco PCA pages cannot be opened or have been defaced, do the following procedure to restore them. Additional troubleshooting information and procedures are available in the “[Cisco Personal Communications Assistant](#)” chapter.

### To Restore the Cisco PCA Files and Applications

- 
- Step 1** On the Cisco Unity server, insert the Cisco Unity disc that contains the cscoserv directory. For example, for the Cisco Unity 4.0(3) release, the cscoserv directory is on Cisco Unity DVD 1 and on Cisco Unity CD 2.
- Step 2** Open a command prompt, and change to your DVD or CD-ROM drive.
- Step 3** Enter `cd cscoserv`.
- Step 4** Enter `setup.js source=“<DVD or CD drive>:\cscoserv\setup.msi” target=“<Cisco Unity drive>:\commserver”`.
- For example, if your DVD or CD-ROM drive is drive D and Cisco Unity is installed on drive C, enter:
- ```
setup.js source=“d:\cscoserv\setup.msi” target=“c:\commserver”
```
- Step 5** Wait a few minutes while the script runs.
- The cscoserv_script.log file is saved to the current user temporary file directory (for example, Documents and Settings\<User>\Local Settings\Temp). You can observe the progress of the script by opening the log file in a browser and refreshing the browser periodically.
- Step 6** When the script has finished running, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 7** Confirm that Tomcat and the World Wide Web Publishing Service are started. If not, restart them. You do not need to restart the Cisco Unity server to implement your changes.
-

Subscribers Cannot Access Cisco Personal Communications Assistant Pages

Subscribers use the Cisco PCA website to access the Cisco Unity Assistant. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.) When a subscriber cannot access the Cisco Personal Communications Assistant (PCA) pages, consider the following possible causes:

URL Is Case-Sensitive

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

Browser Configuration Is Not Correct

When a subscriber cannot access any of the Cisco PCA pages, it may be that the subscriber browser is not configured properly. Make sure that the subscriber browser is configured to:

- Enable Active scripting.
- Download and run ActiveX controls.
- Enable Java scripting.

- Accept all cookies.

For a list of supported versions of Cisco Unity combined with the supported versions of the software on client workstations, refer to the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations*, available at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/clientmx.htm.

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

When Cisco Unity is set up to use SSL, the browser displays a message to alert the subscriber that the authenticity of the Cisco PCA site cannot be verified and therefore, its content cannot be trusted. Subscribers will see this message even if they add the Cisco PCA website to their list of trusted sites for the browser.

To prevent the browser from displaying the security alert, you can:

- Distribute the certificate to the trusted root store for all users in the domain by adding it to the Group Policy. Refer to the “Manually Setting Up Cisco Unity to Use SSL” chapter in the *Cisco Unity System Administration Guide*.
- Tell subscribers how to add the certificate to the trusted root store on their own computers. Refer to the “Setting Up Client Applications” chapter in the *Cisco Unity System Administration Guide*.

The *Cisco Unity System Administration Guide* is available at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.

Discuss the two options with the network administrator for your organization to determine which is best for your site.

Subscribers Cannot Access the Cisco Unity Assistant from the Cisco PCA

When subscribers can access the Cisco PCA, but cannot access the Cisco Unity Assistant, confirm that subscribers have been given the proper class of service rights on the Subscribers > Class of Service > Features Page in the Cisco Unity Administrator.

Note that the Media Master control bar, which appears on the Cisco Unity Assistant pages, is not available across a firewall.

Subscribers Cannot Save Changes on Pages in the Cisco Unity Assistant

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

No Sounds Play on the Multimedia System After Installing the Cisco CallManager Software

When a multimedia system is installed on the Cisco Unity server, registry entries for the multimedia system wave driver may be overwritten when you install the Cisco wave driver. If this happens, the multimedia system no longer plays sounds. Contact Cisco TAC.

Subscribers Cannot Be Located in a New or Updated Directory Handler

Subscribers or outside callers may report that they are unable to locate one or more subscribers in a recently created or updated directory handler. When a directory handler is set to search by a distribution list, the membership is synchronized from the IBM Lotus Notes Directory into the Cisco Unity SQL database. Changing the distribution list that the directory handler searches on requires synchronization. The synchronization takes place when the Cisco Unity directory services (AvDSAD and AvDSGlobalCatalog) poll the directory for any changes to be applied to the SQL database, which usually occurs within 15 to 20 minutes after the change is made on the Directory Handler Search Options page in the Cisco Unity Administrator.

To initiate an immediate synchronization, do the following procedure.

To Manually Synchronize the Cisco Unity Database

-
- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page.
 - Step 2** In the Replicate Cisco Unity Directory Objects section, click **Changed Objects**.
The Settings page is refreshed and the database changes will be synchronized in the background.
 - Step 3** Wait a few minutes, then call in to Cisco Unity to confirm that the subscribers can be located in the directory handler.
 - Step 4** If the subscribers still can not be located, confirm that they have recorded names. Subscribers must have recorded names to be accessed by using directory handlers.
-

Another way to update directory handlers is to change the membership of a distribution list by which one or more directory handlers are scoped. Changes made to distribution list membership by using the Cisco Unity Administrator are updated in the Cisco Unity database within a few minutes. However, in complex networked sites, the replication process may take much longer. This is a function of network complexity and varies from site to site. The network replication process time is not a function of Cisco Unity directory synchronization services, and it is not possible to reduce this time by using the previous procedure.

Cisco Unity Tray Icon Is Missing from the Status Bar

To Manually Start the Cisco Unity Tray Icon

- Step 1** Browse to the CommServer directory.
- Step 2** Run `AvCsTrayStatus.exe`. The tray icon will be restored.
-

Cisco Unity Administrator or Status Monitor Pages Cannot Be Opened or Have Been Defaced

Cisco Unity Administrator Page Cannot Be Accessed After an Upgrade

The following error message may appear after a Cisco Unity upgrade, or application of a Microsoft service pack.

Error Message Access Denied. Your browser must have cookies enabled to access the Unity web pages.

Explanation This error can occur if cookies are not enabled, or if the Cisco Unity server name contains unsupported DNS characters.

Recommended Action Do the following procedure.

To Enable Cookies on the Cisco Unity Server and Confirm the Server Name

- Step 1** In Internet Explorer, click **Tools > Internet Options**.
- Step 2** On the Privacy Tab, Under the Security options for Intranet, confirm that the Settings slide bar is not set to Block All Cookies.
- Step 3** In Internet Explorer, click **Help > About Internet Explorer**. Confirm that the version is 6.0 and that SP1 is installed.
- With SP1, all ASP cookies are blocked if the server name contains non-DNS supported characters, such as an underscore.
- Step 4** On the desktop, right-click **My Computer**, then click **Properties**.
- Step 5** On the Network Identification tab, confirm that the computer name contains only DNS-supported characters. Note that DNS-supported characters include A through Z, a through z, and 0 through 9. The underscore is not supported. If your server name contains non-DNS-supported characters, change the server name to use only DNS-supported characters.
-

Virus Incidents and Hacker Attacks

Virus incidents and attacks from hackers can cause the Cisco Unity Administrator or Status Monitor pages to be defaced or to become unusable. You can restore these pages by doing one of the following:

- Run the Cisco Unity install again. Refer to the *Cisco Unity Installation Guide* for instructions (this guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst403/dom/index.htm).
- Manually restore the applicable files from the Cisco Unity discs by using the following procedure.

To Manually Restore the Cisco Unity Administrator or Status Monitor Pages

For information on restoring defaced or unusable Cisco Personal Communications Assistant (PCA) pages, see the “[Subscribers Cannot Access Cisco Personal Communications Assistant Pages](#)” section on [page 13-5](#).

-
- Step 1** From Cisco Unity Disc 1, copy the **Web** directory to the CommServer directory on the Cisco Unity server. In the Confirm Folder Replace window, click **Yes to All**.
- Step 2** For US English, from Cisco Unity Disc 1, copy the **Localize\Web** directory to the CommServer directory on the Cisco Unity server. In the Confirm Folder Replace window, click **Yes to All**.
- Step 3** For each additional language, locate the Cisco Unity disc on which the language files are stored. Repeat [Step 2](#). In the Confirm Folder Replace window, click **Yes to All**.
-



Reports

About Problems With Reports

Problems and troubleshooting procedures specific to reports are described in this chapter.

A Requested Report Was Not Generated

To Research a Report

- Step 1** In Internet Explorer, browse to **http://<Cisco Unity server name>/status** or double-click the desktop shortcut to the Status Monitor.
- Step 2** In the Status Monitor page, click the **Report Status** icon.
- Step 3** Locate the report you are waiting for in the list of submitted reports. The wait time for a queued report will vary depending on the size of the database and on how busy the system is.
- Step 4** If wait time for the report seems excessive, do one or more of the following:
- Cancel the queued report and request it again at a time when the system is not as busy.
 - Cancel the queued report, refine the selection criteria, and then submit the report again.
 - On the Windows Start menu, click **Programs > Administrative Tools > Services**. Locate **AVRepDirSvrSvc**. If reports are not working properly or are locked, restarting this service will remove the locked state and the reports process will be restarted. Note that some queued reports may be lost due to the restart.
- Step 5** If a requested report is missing from the Report Status page, this may be due to stopping and restarting Cisco Unity or the AvRepDirSvrSvc. Request the report again.
- Step 6** If requested reports are still not being produced, on the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.
- Step 7** On the Cisco Unity Diagnostic Viewer screen, click the **Configure Micro Traces** icon.
- Step 8** Check the check boxes for all traces beginning with the word **Report**.
- Step 9** On the Cisco Unity Diagnostic Viewer screen, click **Start New Log Files**.
- Step 10** Request the reports again at a time when the system is not busy. Wait for a time equal to the wait time previously experienced. If the reports print successfully, skip to [Step 15](#). If the reports do not print, continue with [Step 11](#).

- Step 11** To view the log files, click **Process > AvCsMgr**, and then click the **Current** log file. The selected log file is formatted and displayed in the right pane.
- Step 12** To export or save a copy of the log file, click **Action > Export List**.
- Step 13** Name the file and save it to a location of your choice in .txt or .csv format.
- Step 14** If the requested reports still are not produced, and you are unable to determine the cause of the problem from the diagnostic logs, contact the Cisco Technical Assistance Center (TAC).
- Step 15** To turn off the traces set in [Step 8](#), on the Cisco Unity Diagnostic Viewer screen, click **Disable All Traces**.
-

Related Documentation

- Refer to the “Overview: Reports” section in the “Reports” chapter of the *Cisco Unity System Administration Guide*. The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/dom/index.htm.

Report Notification Not Generated

The Installer account has no mailbox. Therefore, if reports are requested when using the Installer account, no notification will be received when a report is complete. If you are using the Installer account (or another account that has no mailbox) to request reports, you can view the completed reports in the \CommServer\Reports directory.



Cisco Personal Communications Assistant

About Cisco PCA Installation, Repair, and Removal

The Cisco PCA installation uses Windows Installer technology and support scripts (javascript). The installation of the Cisco PCA is an integral part of the Cisco Unity installation process, and therefore, “hidden” from the installer.

If you have the Cisco Unity installation disks, you can restore corrupt or missing Cisco PCA files and applications by running an installation script at a command prompt. When you restore the Cisco PCA, the installation script removes any existing Cisco PCA-related files and applications, including the Tomcat service and its integration to the IIS server.

If you no longer want the Cisco PCA on your Cisco Unity server, another script allows you to safely remove all Cisco PCA files.



Caution

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

About Cisco PCA Logging

When the Cisco PCA is initially installed, the `cscoserv_script.log` is created. The log file contains information about the installation and configuration of the Cisco PCA. When you restore or remove the Cisco PCA by using the `setup.js` and `uninstall.js` scripts, the `cscoserv_script.log` is created or updated. It contains information about the restored or removed installation. The `cscoserv_script.log` is stored in the current user temporary file directory (for example, `Documents and Settings\<User>\Local Settings\Temp`).

Windows Installer automatically provides additional logging. For the initial Cisco PCA installation or for a repaired installation, Windows Installer logs data to the `cscoserv_msi_install.log`; when you remove a Cisco PCA installation, Windows Installer will also log data to the `cscoserv_msi_remove.log`.

Procedures for Troubleshooting the Cisco PCA and Its Components

When the Cisco PCA fails to operate properly, do the following tasks in the order presented:

1. If there is an error message associated with the problem, review the “[Cisco PCA Error Messages](#)” section on page 15-8 or the “[Procedures for Troubleshooting the Media Master Control Bar](#)” section on page 15-9 (as applicable), and then return to this section as needed.
2. Confirm that the CommServer\Cscoserv directory exists on the Cisco Unity server, and that it contains Java2SDK, Tomcat, bin, and ciscopca directories. If any directories are missing, follow the procedures in the “[Restoring the Cisco PCA](#)” section on page 15-2 to fix the problem.
3. Check 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 15-3.
4. Check that the World Wide Web Publishing service is installed and that the service has started. See the “[Verifying That the World Wide Web Publishing Service Is Started](#)” section on page 15-3.
5. Check that IIS and the Cisco PCA components are configured correctly. See the “[Verifying That IIS and the Cisco PCA Components Are Configured Correctly](#)” section on page 15-3.
6. Check that the IIS and Tomcat integration is configured correctly. See the “[Verifying That the IIS and Tomcat Integration Is Configured Correctly](#)” section on page 15-6.

Finally, to restore or remove the Cisco PCA files and applications, see the procedures in the “[Restoring the Cisco PCA](#)” section on page 15-2 or the “[Removing the Cisco PCA](#)” section on page 15-7, as applicable.

Restoring the Cisco PCA

Do the following procedure to restore corrupt or missing Cisco PCA files and applications.



Caution

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

To Restore the Cisco PCA Files and Applications

- Step 1** On the Cisco Unity server, insert the Cisco Unity disc that contains the cscoserv directory. For example, for the Cisco Unity 4.0(3) release, the cscoserv directory is on Cisco Unity DVD 1 and on Cisco Unity CD 2.
- Step 2** Open a command prompt, and change to your DVD or CD-ROM drive.
- Step 3** Enter `cd cscoserv`.
- Step 4** Enter `setup.js source="<DVD or CD drive>\cscoserv\setup.msi" target="<Cisco Unity drive>\commserver"`.

For example, if your DVD or CD-ROM drive is drive D and Cisco Unity is installed on drive C, enter:

```
setup.js source="d:\cscoserv\setup.msi" target="c:\commserver"
```

- Step 5** Wait a few minutes while the script runs.

The cscoserv_script.log file is saved to the current user temporary file directory (for example, Documents and Settings\<User>\Local Settings\Temp). You can observe the progress of the script by opening the log file in a browser and refreshing the browser periodically.

- Step 6** When the script has finished running, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 7** Confirm that Tomcat and the World Wide Web Publishing Service are started. If not, restart them. You do not need to restart the Cisco Unity server to implement your changes.
-

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 server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** In the right pane, locate **Tomcat** and verify that its status is **Started**.
- If the Tomcat service is not listed in the services manager, it is likely that either the Cisco PCA or the Tomcat service failed to install, or that the Tomcat service registration failed. To correct the problem, you will need to restore the Cisco PCA files and applications. See the [“Restoring the Cisco PCA” section on page 15-2](#).
- If the Tomcat service is listed in the services manager, but is not started, right-click it, and click **Start**.
-

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 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**.
- 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 first need to repair the IIS installation. Then restore the Cisco PCA files and applications (see the [“Restoring the Cisco PCA” section on page 15-2](#)).
- If the World Wide Web Publishing service is listed in the services manager but is not started, right-click it, and click **Start**.
-

Verifying That IIS and the Cisco PCA Components Are Configured Correctly

The Cisco PCA depends on the Tomcat service being correctly configured to load the Cisco PCA application upon startup. It also depends on IIS and the Tomcat service being able to communicate. The Tomcat service installation requires Tomcat and Java2SDK. The `jk_nt_service` application handles the

windows service interface for Tomcat, and it requires that the Tomcat service be configured so that the startup and shutdown control port matches its own. The `jk_nt_service.exe` and its configuration file (`wrapper.properties`) are located in the `CommServer\Cscoserv\Windows\Service` directory.

This section contains two procedures. Do the procedures in order to verify that IIS and the Tomcat service are configured correctly. Enter any missing values and correct settings that do not match what is indicated here. Restart IIS and the Tomcat service if you make any corrections, and then check to see whether the Cisco PCA operates properly afterward.

To Verify That IIS Is Configured Correctly

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Right-click <System-name>, and then click **Properties**.
- Step 3** On the Internet Information Services tab, confirm that **WWW Service** is selected in the Master Properties list, and then click **Edit**.
- Step 4** Click the **ISAPI Filters** tab, and click **cpcaflt** from the list of filter names.
- Step 5** In the Details section, verify that the executable is **isapi_redirect.dll** and that its status is **Loaded**. Note that it is not loaded properly if either of the following are true:
- Either no arrow, or a red arrow, is displayed on the left.
 - The Priority is listed as “Unknown.”
- Step 6** If you determined in [Step 5](#) that the `isapi_redirect.dll` executable is not loaded properly, reload it by doing the following sub-steps:
- a. Verify that no other filter is loading the same `.dll` file or a similar file in another location. This can happen when a legacy setting has already used a Tomcat redirector before the current Cisco Unity software was installed.
 - b. Delete the offending duplicate entry (keep the `cpcaflt` entry), and click **Apply**.
 - c. Click **OK** to close the dialog box and return to the Internet Information Services window.
 - d. In the Services Control Panel, stop the Tomcat service.
 - e. Right-click the <System-name>, and click **Restart IIS**.
 - f. Confirm that IIS is set to restart, and click **OK**.
 - g. Verify that the ISAPI filter is loaded by repeating [Step 1](#) through [Step 5](#).
 - h. If the filter is loaded, restart the Tomcat service in the Services Control Panel.
- Step 7** As needed, click **OK** to close any remaining dialog boxes and return to the Internet Information Services window.
- Step 8** Expand <System-name>, and expand **Default Web Site**.
- Step 9** Under Default Web Site, click **Jakarta**, and then verify that **isapi_redirect.dll** is listed in the right pane.
- Step 10** Right-click **Jakarta**, and click **Properties**.
- Step 11** In the Jakarta Properties dialog box, do the following sub-steps:
- a. On the Virtual Directory tab, verify that the Local Path is set to the **CommServer\Cscoserv\Windows\iis\Bin** directory.
 - b. Click the **Directory Security** tab.
 - c. Under Anonymous Access and Authentication Control, click **Edit**.

- d. In the Authentication Methods dialog box, verify that the **Anonymous Access** check box is checked and the **Integrated Windows Authentication** check box is checked.
 - e. Click **OK** to close the Authentication Methods dialog box.
 - f. Click **OK** to close the Jakarta Properties dialog box.
- Step 12** Under Default Web Site, right-click **AvXml**, and click **Properties**.
- Step 13** In the AvXml Properties dialog box, do the following sub-steps:
- a. On the Virtual Directory tab, verify that the Local Path is set to the **\\InetPub\Wwwroot\AvXml** directory.
 - b. Click the **Directory Security** tab.
 - c. Under Anonymous Access and Authentication Control, click **Edit**.
 - d. In the Authentication Methods dialog box, verify that the **Anonymous Access** check box is checked.
 - e. Click **OK** to close the Authentication Methods dialog box.
 - f. Under Secure Communication, click **Edit**. (If the button is greyed out, skip to [Step 14](#).)
 - g. In the Secure Communications dialog box, verify that the **Require Secure Channel (SSL)** check box is unchecked.
 - h. In the Client Certificates section, verify that **Ignore Client Certificates** is selected and the **Enable Client Certificate Mapping** check box is unchecked.
 - i. Click **OK** to close the Secure Communications dialog box.
 - j. In the AvXml Properties dialog box, click **Apply**.
 - k. Click **OK** to close the AvXml Properties dialog box.
- Step 14** Close the Internet Information Services window.
-

To Verify That the Tomcat Service Is Configured Correctly

- Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Windows\Service**.
- Step 2** Use a text editor to open the **wrapper.properties** file.
- Step 3** Verify that the value for **wrapper.tomcat_home** is set to **CommServer\Cscoserv\Tomcat**, which is the Tomcat installation directory.
- The value must be an absolute path (for example, C:\CommServer\Cscoserv\Tomcat).
- Step 4** Verify that the **wrapper.java_home** value is set to **CommServer\Cscoserv\Java2SDK**, which is the java sdk root.
- The value must be an absolute path (for example, C:\CommServer\Cscoserv\Java2SDK).
- Step 5** Close the **wrapper.properties** file.
-

Verifying That the IIS and Tomcat Integration Is Configured Correctly

The IIS and Tomcat integration depends on the proper installation and configuration of the `isapi_redirect.dll` file in IIS. The redirector file is located in `CommServer\Cscoserv\Windows\iis\Bin` directory, and it uses two support files (`uriworkermap.properties` and `workers.properties`), which are located in the `CommServer\Cscoserv\Windows\iis` directory.

This section contains several procedures. Do the procedures in order to verify that the IIS and Tomcat integration is configured correctly. Enter any missing values and correct settings that do not match what is indicated here. Restart IIS and the Tomcat service if you make any corrections, and then check to see whether the Cisco PCA operates properly afterward.

To Verify the IIS and Tomcat Integration Is Configured Correctly

-
- Step 1** On the Cisco Unity server, browse to the directory `CommServer\Cscoserv\Windows\iis`.
- Step 2** Use a text editor to open the `workers.properties` file.
- Step 3** Verify that the value for `workers.tomcat_home` is set to the Tomcat installation directory (for example, `C:\CommServer\Cscoserv\Tomcat`).
- The value must be the absolute path to the root of the Tomcat installation directory.
- Step 4** Verify that the `workers.java_home` value is set to a proper java sdk root (for example, `C:\CommServer\Cscoserv\Java2SDK`).
- The value must be the absolute path to the root of a Java 2 SDK version 1.3 or later.
- Step 5** Close the `workers.properties` file.
- Step 6** Use the text editor to open `uriworkermap.properties`.
- Step 7** Verify that the file contains the following:
- `/ciscopca=$(default.worker)`
 - `/ciscopca/*=$(default.worker)`
 - `default.worker=ajp13`
- Step 8** Close the `uriworkermap.properties` file.
-

To Verify That the Tomcat Server Is Configured Correctly

-
- Step 1** On the Cisco Unity server, browse to the directory `CommServer\Cscoserv\Tomcat\Webapps`.
- Step 2** Verify that the directory contains the `ciscopca.xml` file. If it does, use a text editor to open it.
- Step 3** Verify that the file contains `<Context path="/ciscopca">`. This defines the Cisco PCA application profile.
- Step 4** Verify that the value for the path attribute is `"/ciscopca"` and the `docBase` attribute is the absolute path to the `ciscopca` directory (for example, `C:\CommServer\Cscoserv\Ciscopca`).
- Step 5** Verify that the value for the `reloadable` attribute is `"False"`. The value controls whether Tomcat forces the Cisco PCA to reload when files change.
- Step 6** Verify that the value for the `debug` attribute is `"0"`. The value sets minimal logging.
- Step 7** Verify that the value for the `privileged` attribute is `"True"`.

- Step 8** Verify that the file contains the “<Logger></Logger>” object declaration within the ciscopca “<Context ></Context>” declaration. The value indicates where engine events are logged for the Cisco PCA.
- Step 9** Close the **ciscopca.xml** file.
-

To Verify That the Cisco PCA Web Application Is Configured Correctly

- Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Ciscopca\WEB-INF**.
- Step 2** Use a text editor to open the **web.xml** file.
- Step 3** Find **unityurl** and verify that the value enclosed by “<param-value id=’unityurl’>” and “</param-value>” is a valid IP address or DNS name for the Cisco Unity server that is hosting the AvXml web service/portal.
- The value cannot be either of the following:
- 127.0.0.1
 - “localhost”
- Step 4** Close the **web.xml** file.
-

Removing the Cisco PCA

Do the following procedure if you no longer want the Cisco PCA files and applications on your Cisco Unity server.



Caution

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

To Remove the Cisco PCA Files and Applications

- Step 1** On the Cisco Unity server, open a command prompt.
- Step 2** Enter **uninstall.js**, and press **Enter**.
- Step 3** Wait a few minutes while the script runs.
- The **cscoserv_script.log** file is saved to the current user temporary file directory (for example, Documents and Settings\<User>\Local Settings\Temp). You can observe the progress of the script by opening the log file in a browser and refreshing the browser periodically.
- You do not need to restart the Cisco Unity server to implement your changes.
-

Cisco PCA Error Messages

Problems that subscribers can experience when logging on to the Cisco PCA, when using the Cisco Unity Assistant, or when using the Cisco Unity Inbox are listed below, along with possible causes for the problems and troubleshooting tips for resolving each issue. Some errors have more than one possible cause. The recommended actions are listed after each cause, and are offered in the suggested order of completion.

Error Message Unable to contact server.

Possible Cause The Cisco Unity server is down, or a network connection has failed.

Recommended Action Confirm that the Cisco Unity server is running, and that all network connections are functioning properly. Restart the Cisco Unity server, as necessary. To verify that the problem is caused by a Cisco Unity server or a network failure, you can change the “unityurl” configuration setting to point to a Cisco Unity server that is running, and then restart the Tomcat service.

Possible Cause AvXml directory security is not set correctly in IIS; Anonymous access may be disabled or secure connections may be enabled.

Recommended Action To correct directory security settings, see the [“Verifying That IIS and the Cisco PCA Components Are Configured Correctly” section on page 15-3](#). Anonymous access should be enabled and secure connections should be disabled.

Error Message Unknown authentication provider.

Possible Cause Jakarta directory security is not set correctly in IIS; the Anonymous Access or Integrated Windows Authentication check boxes may not be checked.

Recommended Action To correct directory security settings, see the [“Verifying That IIS and the Cisco PCA Components Are Configured Correctly” section on page 15-3](#). Both the Anonymous Access and Integrated Windows Authentication check boxes should be checked.

Error Message Site is unavailable.

Symptom The error occurs when a subscriber browses to `http://<Cisco Unity server>/ciscopca`, and when Internet connection issues, a firewall, or SSL restrictions are not factors.

Possible Cause ISAPI redirection filter failed to load.

Recommended Action Do [Step 1](#) through [Step 5](#) in the [“To Verify That IIS Is Configured Correctly” section on page 15-4](#). If the problem is still not resolved, restore the Cisco PCA by doing the procedure in the [“Restoring the Cisco PCA” section on page 15-2](#).

Possible Cause The Tomcat service is stopped.

Recommended Action See the [“Verifying That the Tomcat Service Is Installed and Started” section on page 15-3](#).

Possible Cause The IIS and Tomcat integration is not configured correctly.

Recommended Action See the [“Verifying That the IIS and Tomcat Integration Is Configured Correctly”](#) section on page 15-6.

Procedures for Troubleshooting the Media Master Control Bar

Problems that subscribers can experience when using the Media Master control bar in the Cisco Unity Assistant or Cisco Unity Inbox are listed below, along with possible causes and troubleshooting tips for resolving each issue. Some problems have more than one possible cause. The recommended actions are listed after each cause, and are offered in the suggested order of completion.

Symptom The play and record buttons are greyed out on the Media Master control bar.

Possible Cause The Media Master control bar may not be able to locate the Cisco Unity server because the CommServer\Cscoserv\Ciscopca\WEB-INF\Web.xml “unityurl” setting contains either the 127.0.0.1 IP address or the “localhost” host name, rather than a network IP address or a valid DNS name. (Note that occasionally the “unityurl” setting does contain a valid DNS name, but the symptom is still exhibited. In all cases, however, when “pinging” the IP address for the Cisco Unity server from the subscriber workstation fails, the buttons will appear greyed out on the Media Master control bar.)

Recommended Action Replace the unityurl value with a proper IP address or DNS name, as necessary. Then restart the Tomcat service. See [Step 3](#) in the [“To Verify That the Cisco PCA Web Application Is Configured Correctly”](#) section on page 15-7.

Possible Cause The AvMMPProxySvr service is not started or is down.

Recommended Action Restart the AvMMPProxySvr service.

Possible Cause Network configuration is interfering with COM/DCOM operations.

Recommended Action Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server.

Recommended Action Verify that there is no firewall between the subscriber workstation and the Cisco Unity server. The Media Master control bar does not work through a firewall.

Recommended Action Disable virus-scanning services and VPN client software on the subscriber workstation, as applicable.

Symptom The Media Master control bar does not play or does not record when the subscriber specifies the computer multimedia devices as the playback and recording device, and the multimedia devices work properly otherwise.

Possible Cause Network configuration is interfering with COM/DCOM operations.

Recommended Action Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server.

Recommended Action Verify that there is no firewall between the subscriber workstation and the Cisco Unity server. The Media Master control bar does not work through a firewall.

Recommended Action Disable virus-scanning services and VPN client software on the subscriber workstation, as applicable.

Recommended Action Verify that the AvCsMgr and AvCsGateway services are running as a distinguished Cisco Unity account (as specified during installation) and not the Local System account.

Possible Cause The recording(s) that the Media Master control bar will not play are recorded in the G729a format.

Recommended Action Verify that the subscriber has the G729a codec installed on the workstation, and that the recording(s) will still not play. If this is the case, refer to caveat CSCeb21978 for more information. Bug Toolkit is available at

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Symptom The Media Master control bar does not play or does not record when the subscriber specifies the phone as the playback and recording device.

Possible Cause Network configuration is interfering with COM/DCOM operations.

Recommended Action Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server.

Recommended Action Verify that there is no firewall between the subscriber workstation and the Cisco Unity server. The Media Master control bar does not work through a firewall.

Recommended Action Disable virus-scanning services and VPN client software on the subscriber workstation, as applicable.

Recommended Action Verify that the AvCsMgr and AvCsGateway services are running as a distinguished Cisco Unity account (as specified during installation) and not the Local System account.



Cisco Unity Services and Their Functions

Cisco Unity Services are the top level components for the diagnostic traces that are used in troubleshooting. When a diagnostic trace is viewed by using the Cisco Unity Diagnostic Tool, the file always contains the Service in the file name immediately following the “diag_”.

Table A-1 Cisco Unity Services


Service	Function
AvCsGateway	The Gateway service provides a secure interface to the Manager (AvCsMgr) service. It allows external processes to query the state of the Manager, start or stop the Manager, or request internal interfaces to the Manager components (if allowed).
AvCsMgr	The Manager service is the primary Cisco Unity service and the core voice messaging system. It runs the CommServer platform components, provides status on the components, and exposes component interfaces to other internal and external components.
AvDirChangeWriter	The Directory Change Writer service gets messages from the change queue (posted by the AvDSDomino service) and writes them to the Cisco Unity SQL database.
AvDSDomino	The Domino Datastore service monitors the Cisco Unity SQL database for changes in Cisco Unity objects (users, locations, distribution lists, contacts) and sends notification of the changes to the Change Writer service. This keeps Cisco Unity synchronized with directory changes made in the Cisco Unity Administrator.
AvGaenSvr	<p>The Event Notification utility service polls the Event log and sends e-mail and/or voice mail notifications according to the Event Properties set in the Event Notification Utility Administrator.</p> <p> Caution We recommend that you use the Event Monitoring System instead of the Event Notification utility.</p>
AvLic	The Licensing service provides secure licensing information to Cisco Unity and authenticated clients. In addition, it monitors the Cisco Unity SQL database and provides dynamic utilization information of per-seat licensing features.
AvMMProxySvr	The Media Master Proxy server provides client authentication and anonymous access to media and resource interfaces. Available to anyone, this service provides application-level authentication of clients running on any platform. After authenticating, it then exposes interfaces for streaming WAV files over the phone or to a client platform.
AvMsgStoreMonitorSvr	The Message Store Monitor service watches subscriber mailboxes on the Cisco Unity server for new or deleted messages. This service then adds an MWI request to the Notifier Queue to turn the subscriber message waiting indicator (MWI) on or off. When message notification is enabled, this service adds events for message notifications through pager or message delivery.

Table A-1 Cisco Unity Services (continued)

Service	Function
AvNotifierMgr	The Notifier Manager provides notification for MWIs and event notifications through the Notifier and NotifyQ components.
AvSqlChangeWriter	The SQL Change Writer service monitors the Cisco Unity SQL database and requests the applicable directory service to update the directory as needed.
AvTtsSvr	The Text to Speech service provides a text-to-audio rendering service that is used by the Call Control/Media (Miu) component to play e-mail messages over the phone.
AvUMRSyncSvr	When the message store is not functioning, The Unity Messaging Repository (UMR) service places voice messages left by unidentified callers—an outside caller or a caller from inside the organization calling from a phone that is not associated with a subscriber account (such as a conference room)—in the UnityMTA directory. UMR lets subscribers listen to these messages and gives them to the message store when it begins functioning again.
CsBridgeConnector	The Connector service monitors the UOmni mailbox and synchronizes directory information in both directions between Cisco Unity and an Octel Node (the Bridge).
CsEmsSvc	The Event Monitoring Service polls the Event log and sends e-mail and/or voice mail notifications according to the settings for the events and recipients in the Event Monitoring Service window.

Behavior of Cisco Unity Services in a Configuration with Domino

Services that log on with the account that owns the Cisco Unity directory and message store services are listed as logging on as UnitySvc, the suggested Active Directory user logon name.

Table A-2 Behavior of Cisco Unity Services in a Configuration with Domino

Service	Dependencies	Startup Mode	Logs on as	Comments
AvCsGateway	MSSQLSERVER	Automatic	UnitySvc	Critical; must be restarted if stopped. Starts and stops AvCsMgr.
AvCsMgr	Dialogic System Service, MSSQLSERVER, Telephony	Manual	UnitySvc	Critical; started and stopped by the system tray or the Status Monitor via AvCsGateway. Can be started only by AvCsGateway; should be stopped by AvCsGateway. If AvCsGateway is started by the Status Monitor, AvCsMgr is also started.
AvDirChangeWriter	Message Queuing, MSSQLSERVER	Automatic	Local system account (needs access to SQL)	Critical, must be restarted if stopped. If stopped, there is no impact on AvCsMgr.

Table A-2 Behavior of Cisco Unity Services in a Configuration with Domino (continued)

Service	Dependencies	Startup Mode	Logs on as	Comments
AvDSDomino	MSSQLSERVER, message queuing	Automatic	UnitySvc	Critical, must be restarted if stopped.
AvGaenSvr	None	Disabled	UnitySvc	Not critical. If stopped, there is no impact on AvCsMgr.
AvLic	MSSQLSERVER	Automatic	Local system account	
AvMMPProxySvr	Remote Procedure Call (RPC)	Automatic	Local system account	Critical; used by web applications and e-mail clients.
AvMsgStoreMonitorSvr	None	Manual	UnitySvc	Critical; used for message notification and MWIs.
AvNotifierMgr	None	Manual	UnitySvc	Critical; used for message notification and MWIs.
AvSqlChangeWriter	MSSQLSERVER	Automatic	Local system account	Runs during the MSCW bulk synchronization of all SQL and AD data.
AvTtsSvr	None	Manual	Local system account	Not critical.
AvUMRSyncSvr	MSSQLSERVER	Manual	UnitySvc	Critical; must be restarted if stopped; AvCsMgr starts UMR during startup if UMR is not already running. If stopped, there is no impact on AvCsMgr, but cannot store messages if the Domino server is down; must be restarted if stopped.
CsBridgeConnector <i>(always installed, but started only if the Bridge is licensed)</i>	MSSQLSERVER	Manual	UnitySvc	Not critical; can be disabled if the Bridge is not used; does not start if no Bridge ports are licensed. If stopped, there is no impact on AvCsMgr, but the Bridge does not function.
CsEmsSvc	None	Manual	UnitySvc	Not critical. If stopped, there is no impact on AvCsMgr.



A

- access code, missing for external line [8-6](#)
- account, locked [10-5](#)
- ActiveAssistant. See Cisco Unity Assistant
- AGC [6-7](#)
- Application logs, finding errors [10-2](#)
- audio not transmitted [9-1](#)
- audio quality [6-1](#)
- automatic gain control [6-7](#)

B

- browser error messages [10-3](#)
- busy ports notification [10-5](#)

C

- callers hear reorder tone or dead air space [3-3](#)
- calls
 - disconnected [5-4](#)
 - internal, not answered [3-5](#)
 - none answered [3-1](#)
 - some answered [3-5](#)
- call transfers, transferred to incorrect greeting [4-1](#)
- Call Viewer utility, about [12-10](#)
- Cisco CallManager integration
 - diagnostic test setup [1-1](#)
 - multimedia sound system problems [13-7](#)
 - subscriber transfer problems [4-3](#)
- Cisco CallManager phone system, DTMF signal problems [13-2](#)
- Cisco Personal Communications Assistant

- about installation [15-1](#)
- access problems [13-5](#)
 - logging [15-1](#)

Cisco TAC, reporting problems to [1-3](#)

Cisco Unity Administrator, access problems [13-9](#)

Cisco Unity Assistant

- access problems [13-6](#)
- missing or unusable pages [13-4](#)

class of service

- license limit reached [10-4](#)
- logon access denied [10-3](#)

codecs, changing [6-5](#)

comfort noise [6-10](#)

COM ports

- disabling device detection [3-3](#)
- viewing assignments [3-2](#)

confirming

- phone system settings [3-2](#)
- ports, number of [3-8](#)

conversation errors [10-5](#)

D

data packets, viewing [12-1](#)

dead air space, callers hear [3-3](#)

delayed messages, causes of [5-1](#)

diagnostics test setup [1-1](#)

Diagnostic Tool [12-11](#)

Dialogic

automatic gain control [6-9](#)

quiet parameter, changing [5-4](#)

single-line test setup [1-2](#)

dial tone present at end of message [5-5](#)

directory handler missing subscribers [13-7](#)

disabling

- COM ports [3-2](#)
- detection of devices on COM ports [3-3](#)
- diagnostic logs [12-11](#)
- Found New Hardware wizard for voice-fax cards [9-3](#)

disconnected calls [5-4](#)

distribution list missing subscribers [13-7](#)

Dr. Watson logs, obtaining [2-2](#)

DTMF

- duration and delay settings, comparing [13-4](#)
- phone signal problems (circuit-switched phone systems) [13-3](#)
- phone signal problems (Cisco CallManager) [13-2](#)
- testing on feature-set phones [13-3](#)
- testing on operator console [13-3](#)

dual network interface card configuration [9-2](#)

E

e-mail

- attachments, fax problems [11-1](#)
- Text to Speech problems [10-6](#)

error messages

- browser [10-3](#)
- e-mail and voice [10-5](#)
- startup [10-1](#)
- Windows [10-3](#)

errors, finding in Application and System Event logs [10-2](#)

Event log traces, obtaining [2-2](#)

external lines

- access code missing [8-6](#)
- use in message notification [8-5](#)

F

fax

- delivery problems [11-2](#)

- e-mail attachment, problems [11-1](#)
- forwarded [11-2](#)
- verifying subscriber settings [11-1](#)

feature set phones, DTMF signal problems [13-3](#)

forward timer, out of synch [4-2](#)

Found New Hardware wizard, disabling for voice-fax cards [9-3](#)

G

gain control [6-7](#)

garbled TTY characters [6-10](#)

greetings

- call transfer problems [4-1](#)
- volume [6-1](#)
- wrong greeting plays [4-3](#)

H

hacker attack, recovery from [13-4, 13-9](#)

hunt groups

- programming errors [3-6](#)

I

Integration Monitor

- correcting display problems [12-4](#)
- display options table [12-3](#)
- field value table [12-2](#)
- frequently asked questions [12-4](#)
- utility, about [12-1](#)

integrations

- call transfer problems [4-1](#)
- internal calls, not answered [3-5](#)
- test setup, single-line [1-2](#)
- verifying settings (Cisco CallManager) [4-3](#)

L

Learn Tones

- process failure, troubleshooting [12-9](#)
- running [5-5](#)
- switch configuration file location [12-6](#)
- tone definitions [12-5](#)
- utility, about [12-5](#)

licensing problems [3-8](#)

log files

- and traces [2-1](#)
- creating [12-11](#)

Mmacro traces [12-11](#)median volume setting [6-9](#)

message notifications

- access code errors [8-6](#)
- device problems [8-6](#)
- dual integration settings, correcting [8-7](#)
- external numbers, no calls made [8-5](#)
- port setup [8-2](#)
- setup, testing [8-3](#)
- slow for multiple subscribers [8-1](#)
- slow for single subscriber [8-3](#)
- subscriber errors [8-4](#)
- testing devices [8-7](#)

message playback volume [6-1](#)

messages

- delayed [5-1](#)
- disappearing [5-2](#)
- notifications, types that trigger [8-6](#)
- playback volume problems [6-1](#)
- recording cuts off [5-3](#)

messaging waiting indicators (MWIs)

- about [7-1 to 7-4](#)
- troubleshooting [7-4 to 7-12](#)

micro traces diagnostic tool [12-11](#)Miu diagnostics [2-2](#)multimedia sound system problems [13-7](#)

MWIs. See message waiting indicators

Nnetwork interface card (NIC) [9-1](#)**O**

opening greeting

- caller hears in error (Cisco CallManager integration) [4-3](#)
- caller hears instead of personal options [13-2](#)

Ppackets, viewing values [12-1](#)

PCA. See Cisco Personal Communications Assistant

phone system

- line not working [3-9](#)
- packets, viewing [12-1](#)
- programming, confirming (Ericsson MD-110) [4-3](#)
- settings, confirming [3-2](#)

port configuration

- confirming [3-8](#)
- disabled or set incorrectly [3-8](#)
- licensing does not match [3-8](#)
- message notification problems [8-2](#)

ports

- all ports busy notification [10-5](#)
- assigned incorrectly [3-2](#)
- calls misdirected [3-8](#)
- calls sent to port that is not set to answer [8-2](#)
- confirming number [3-8](#)
- disabled or enabled [3-8](#)
- hanging due to misconfiguration [8-2](#)

prompts, sound quality issues [6-10](#)

Q

quiet parameter, Dialogic voice card [5-4](#)

R

Registry, using to enable ports [3-9](#)

reorder tone

callers hear [3-3](#)

hearing, at end of message [5-5](#)

hearing, when answering call [4-3](#)

repeat notifications [8-4](#)

reports

generation problems [14-1](#)

notification problems [14-2](#)

restart notifications [8-4](#)

ring signal, testing [3-5](#)

rings to wait, setting [4-3](#)

routing rules, testing [3-7](#)

S

services, Cisco Unity [A-1](#)

service startup settings, checking [10-2](#)

Set Record Format utility [6-5](#)

Set Volume utility [6-2](#)

single-line tests, setup [1-2](#)

Skippy TSP traces, obtaining [2-4](#)

startup problems

browser error messages [10-3](#)

error messages [10-1](#)

Status Monitor

accessing after upgrade [10-4](#)

access problems [13-9](#)

missing or unusable pages [13-9](#)

subscribers

conversation problems [13-2](#)

create user error [9-2](#)

missing from directory handler [13-7](#)

missing from distribution list [13-7](#)

supervised transfers, confirming settings [4-2](#)

Switch.ini version, locating [1-5](#)

System Event logs, finding errors [10-2](#)

system event notifications [10-6](#)

T

test extensions, setting up [1-1](#)

testing

DTMF signals on feature-set phones [13-3](#)

DTMF signals on operator console [13-3](#)

hunt group programming (non-IP phone systems) [3-6](#)

routing rules [3-7](#)

touchtones, no response to [13-2](#)

traces

macro [12-11](#)

micro [12-11](#)

TSP [2-4](#)

TSP version number, locating [1-5](#)

TTY garbled characters [6-10](#)

U

Universal Dialogic Diagnostics utility [12-14](#)

utilities

Advanced Settings Tool [12-13](#)

AudioStat [6-11](#)

Call Viewer [12-10](#)

CAP Ripper [6-13](#)

Cisco Unity Diagnostic Tool [12-11](#)

Integration Monitor [12-1](#)

Learn Tones [12-5](#)

RTP Parser [6-14](#)

Set Record Format [6-5](#)

Set Volume [6-2](#)

Universal Dialogic Diagnostics [12-14](#)

Wave Gain [6-6](#)

V

verifying

- fax settings, subscriber [11-1](#)

- integration settings, Cisco CallManager [4-3](#)

virus, recovery from [13-4, 13-9](#)

voice cards

- Dialogic, testing with UDD utility [12-14](#)

- problems, isolating [3-9](#)

voice-fax cards, disabling Found New Hardware wizard [9-3](#)voice not transmitted [9-1](#)

voice server

- hard disk almost full errors [10-6](#)

- restarting [10-7](#)

volume, greetings and voice names [6-1](#)

WWave Gain utility [6-6](#)web pages missing or unusable [13-4, 13-9](#)

