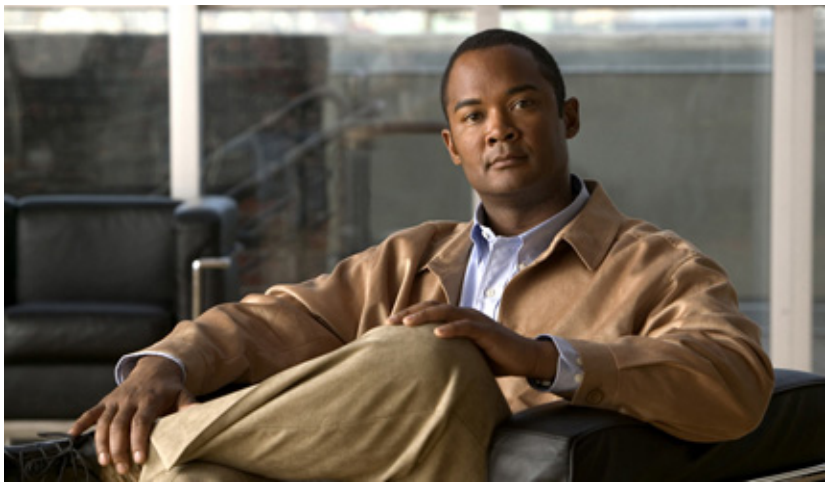

Troubleshooting Guide for Cisco Unity Connection

Release 9.x
Revised September 2013

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

Text Part Number:

Troubleshooting Guide for Cisco Unity Connection Release 9.x

CONTENTS

Preface

Audience and Use

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

Documentation Conventions

Table 1 Troubleshooting Guide for Cisco Unity Connection Conventions

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Select **OK**.) • Information that you enter. (Example: Enter **Administrator** in the Username box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping <IP address>**.)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, select **Settings > Control Panel > Phone and Modem Options**.)

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

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

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

Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 9.x*. The document is shipped with Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/roadmap/9xcucdg.html.

Documentation References to Cisco Unified Communications Manager Business Edition

In the Cisco Unity Connection 9.x documentation set, references to "Cisco Unified Communications Manager Business Edition" and "Cisco Unified CMBE" apply to both Business Edition version 9.0 and to Business Edition 5000 versions 9.x. The references do not apply to Business Edition 6000.

Obtaining Documentation and Submitting a Service Request

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

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

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

Cisco Product Security Overview

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

A summary of U.S. laws governing Cisco cryptographic products may be found at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance, contact us by sending email to export@cisco.com.

CHAPTER 1

Overview of Cisco Unity Connection 9.x Troubleshooting

The *Troubleshooting Guide for Cisco Unity Connection* helps you resolve problems that you might encounter with Connection. If your Connection system is exhibiting a symptom that is documented in this troubleshooting guide, perform the recommended troubleshooting procedures. However, if the symptom is not documented in this troubleshooting guide, or if the recommended troubleshooting does not resolve the problem, do the following procedure to determine whether the problem might be caused by SELinux Security policies. (SELinux replaced Cisco Security Agent(CSA) on Connection servers.)

To Troubleshoot Symptoms that Cannot Be Resolved by Documented Troubleshooting Procedures

Step 1 To check the status of SELinux on Connection server, run the Command Line Interface (CLI) command **utils os secure status**.

Step 2 If SELinux is in Enforcing mode, run the CLI command **utils os secure permissive** to put the Connection server in Permissive mode. For more information on the CLI command **utils os secure permissive**, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 3 Try to reproduce the symptom with SELinux in permissive mode. If the symptom is reproducible, it is not caused by SELinux.

Step 4 If the symptom is not reproducible, do the following steps to gather logs before you contact Cisco TAC:

a. Create your test directory on sftp server to save the audit log diagnostic file at that location.

b. Put Connection server in Enforcing mode by running the CLI command **utils os secure enforce**.

c. Try to create the symptom again.

d. Create the audit logs diagnostic file by running the CLI command **utils create report security**. This command creates a diagnostic file “security-diagnostics.tar.gz”. Copy the diagnostic file to sftp directory created in step 4(a) by running the CLI command **file get activelog syslog/security-diagnostics.tar.gz**. For more information on the CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 5 Contact Cisco TAC.

For example, to troubleshoot the switch version failures as part of upgrade from Unity Connection 8.6 to a later version, do the following procedure.

To Troubleshoot Switch Version Failures As Part of Upgrade from Cisco Unity Connection 8.6 to a Later Version

Step 1 To check the status of SELinux on Connection server, run the Command Line Interface (CLI) command **utils os secure status**.

Step 2 If SELinux is in Enforcing mode, run the CLI command **utils os secure permissive** to put the Connection server in Permissive mode. For more information on the CLI command **utils os secure permissive**, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 3 Retry the switch version with SELinux in permissive mode. If the switch version failure is reproducible, it is not caused by SELinux.

Step 4 If the switch version failure is not reproducible, do the following steps to gather logs before you contact Cisco TAC:

a. Create your test directory on sftp server to save the audit log diagnostic file at that location.

b. Put Connection server in Enforcing mode by running the CLI command **utils os secure enforce**.

c. Try to create the symptom again.

d. Create the audit logs diagnostic file by running the CLI command **utils create report security**. This command creates a diagnostic file "security-diagnostics.tar.gz". Copy the diagnostic file to sftp directory created in step 4(a) by running the CLI command **file get activelog syslog/security-diagnostics.tar.gz**. For more information on the CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 5 Contact Cisco TAC.

To Troubleshoot Failsafe Message While Upgrading from Connection 8.6.(x)

If you are getting the failsafe message while upgrading from Connection 8.6.(x) in a cluster, put the system in the permissive mode using the CLI command **utils os secure permissive** command until the switch version process is completed. For more information on the CLI command used to put the system in permissive mode, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

CHAPTER 2

Diagnostic Traces in Cisco Unity Connection 9.x

Diagnostic traces can be used as a tool to assist you in troubleshooting problems. In Cisco Unity Connection Serviceability, you enable traces to troubleshoot Cisco Unity Connection components. In Cisco Unified Serviceability, you enable traces to troubleshoot services that are supported in Cisco Unified Serviceability. After the traces are enabled, you can access the trace log files by using Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

See the following sections:

Traces in Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x

Cisco Unity Connection Serviceability provides both micro traces and macro traces that you can enable individually or in any combination.

Cisco Unity Connection Serviceability micro traces	Used to troubleshoot problems with specific Cisco Unity Connection components.
Cisco Unity Connection Serviceability macro traces	Used to troubleshoot general areas of Cisco Unity Connection functionality.

After the traces are enabled, you can access the trace log files by using the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

See the following sections:

Cisco Unity Connection Serviceability Micro Traces for Selected Problems

You can use Cisco Unity Connection Serviceability micro traces to troubleshoot problems with specific Cisco Unity Connection components. After the traces are enabled, you can access the trace log files by using the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

Table 2-1 lists the information for Cisco Unity Connection Serviceability micro traces that you need for troubleshooting selected problems and for viewing the trace logs. (For instructions on using Cisco Unity Connection Serviceability micro traces, see the "Using Traces" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.)

Note Enabling Cisco Unity Connection Serviceability micro traces decreases system performance. Enable traces only for troubleshooting purposes.

Table 2-1 Cisco Unity Connection Serviceability Micro Traces for Selected Problems

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
Audio Issues			
Playing an attachment via the TUI	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	ConvSub (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Calendar Integration Issues			
Calendar integration	CCL (levels 10, 11, 12, 13)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsWebDav (levels 10, 11, 12, 13)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
Calendar integration (event notifications)	CsWebDav (levels 10 through 13)	Connection IMAP Server	diag_CuImapSvr_*.uc
Call Issues			
Routing rules	Arbiter (levels 14, 15, 16)	Connection Conversation Manager	diag_CuCsMgr_*.uc
	RoutingRules (level 11)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Client Issues			

Table 2-1 Cisco Unity Connection Serviceability Micro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
Cisco Unified Personal Communicator client (IMAP-related issues) (see also "Cisco Unified Personal Communicator client (IMAP-related issues)" in Table 2-2)	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsMalUmss (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CuImapSvr (all levels)	Connection IMAP Server	diag_CuImapSvr_*.uc
	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
ViewMail for Outlook (sending and receiving messages) (see also "ViewMail for Outlook (sending and receiving messages)" in Table 2-2)	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsMalUmss (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CuImapSvr (all levels)	Connection IMAP Server	diag_CuImapSvr_*.uc
	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
Connection Cluster Issues			
Connection clusters (except file replication)	SRM (all levels)	Connection Server Role Manager	diag_CuSrm_*.uc
Connection cluster file replication	CuFileSync (all levels)	Connection File Syncer	diag_CuFileSync_*.uc
External Message Store Issues			
Accessing emails in an external message store	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
Fax Issues			
File rendering	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
SMTP messages are not sent	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc

Table 2-1 Cisco Unity Connection Serviceability Micro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
SMTP server mishandles faxes	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
LDAP Issues			
LDAP synchronization (see also "LDAP synchronization" in Table 2-3)	CuCmDbEventListener	Connection CM Database Event Listener	diag_CuCmDbEventListener_*.uc
Message Issues			
Dispatch messages (see also "Dispatch messages" in Table 2-2)	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
IMAP messages (see also "IMAP messages"in Table 2-2)	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsMalUmss (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CuImapSvr (all levels)	Connection IMAP Server	diag_CuImapSvr_*.uc
	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
Message delivery and retrieval (see also "Message delivery and retrieval" in Table 2-2)	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsMalUmss (levels 10, 14, 18, 22, 23, 26)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
	Notifier (all levels except 6 and 7)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
	UmssSysAgentTasks (all levels)	Connection System Agent	diag_CuSysAgent_*.uc

Table 2-1 Cisco Unity Connection Serviceability Micro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
NDRs (see also "NDRs" in Table 2-2)	CML (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CuCsMgr (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Notifications not sent (see also "Notifications not sent" in Table 2-2)	CuCsMgr (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
	Notifier (all levels except 6 and 7)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
Secure message aging	UmssSysAgentTasks (all levels)	Connection System Agent	diag_CuSysAgent_*.uc
SMS notifications	Notifier (all levels except 6 and 7)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
Networking Issues			
Intrasite Networking replication (see also "Intrasite Networking replication" in Table 2-2)	CuReplicator	Connection Digital Networking Replication Agent	diag_CuReplicator_*.uc
Intersite Networking replication	Feeder (levels 00, 01, 02, 03)	Connection Tomcat Application	diag_Tomcat_*.uc
	FeedReader (levels 00, 01, 02, 03, 10, 14)	Connection System Agent	diag_CuSysAgent_*.uc
VPIM message delivery (see also "VPIM message delivery" in Table 2-2)	MTA (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
Personal Call Transfer Rule Issues			
Accessing calendar information	CCL (levels 10, 11, 12, 13)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
	CsWebDav (levels 10, 11, 12, 13)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc

Table 2-1 Cisco Unity Connection Serviceability Micro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
Configuring personal call transfer rule settings by phone	ConvSub (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Rule processing during calls to a rules-enabled user	ConvRoutingRules (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
	RulesEngine (all levels)	Connection Tomcat Application	diag_Tomcat_*.uc
		Connection Conversation Manager	diag_CuCsMgr_*.uc
Rules-related conversations	CDE (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Phone View Issues			
Phone View	PhoneManager (all levels)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Report Issues			
Data collection in reports	ReportDataHarvester (all levels)	Connection Report Data Harvester	diag_CuReportDataHarvester_*.uc
Display of reports	CuService (all levels)	Connection Tomcat Application	diag_Tomcat_*.uc
RSS Feed Issues			
Access to RSS feeds of voice messages	RSS (all levels)	Connection Tomcat Application	diag_Tomcat_*.uc
SNMP Issues			
SNMP	CuSnmpAgt (all levels)	Connection SNMP Agent	diag_CuSnmpAgt_*.uc
SpeechView Transcription Issues			
SpeechView transcriptions	SttClient (all levels)	Connection Message Transfer Agent	diag_MTA_*.uc
	SttService (all levels)	Connection SpeechView Processor	diag_SttService_*.uc
	SMTP (all levels)	Connection SMTP Server	diag_SMTP_*.uc
	MTA (level 10, 11, 12, 13)	Connection Message Transfer Agent	diag_MTA_*.uc
	SysAgent (level 10, 11, 12, 16)	Connection System Agent	diag_CuSysAgent_*.uc
Sending transcriptions to notification devices	Notifier (level 16, 21, 25, 30)	Connection Notifier	diag_CuNotifier_*.uc
Test Button (External Service and External Service Account) Issues			
Test button (external service diagnostic tool)	CuESD (all levels)	Connection Tomcat Application	diag_Tomcat_*.uc
Web Inbox Issues			
Interactions with Representational State Transfer (REST) API	VMREST (all levels)	Connection Tomcat Application	diag_Tomcat_*.uc

Cisco Unity Connection Serviceability Macro Traces for Selected Problems

Cisco Unity Connection Serviceability macro traces enable a preselected set of Cisco Unity Connection Serviceability micro traces with which you can troubleshoot general areas of Cisco Unity Connection functionality.

Table 2-2 lists the information for Cisco Unity Connection Serviceability macro traces that you need for troubleshooting selected problems and for viewing the trace logs. (For instructions on using Cisco Unity Connection Serviceability macro traces, see the "Using Traces" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.)

Note Enabling Cisco Unity Connection Serviceability macro traces decreases system performance. Enable traces only for troubleshooting purposes.

Table 2-2 Cisco Unity Connection Serviceability Macro Traces for Selected Problems

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
Audio Issues			
Audio quality	Media (Wave) Traces	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Mixer	diag_CuMixer_*.uc
Call Issues			
Call control	Call Control (Miu) Traces (expand the macro trace to select SIP or SCCP)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Call flow	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
ViewMail for Outlook (recording or playback by phone)	Call Control (Miu) Traces (expand the macro trace to select SIP or SCCP)	Connection Conversation Manager	diag_CuCsMgr_*.uc
Client Issues			
Cisco Unified Personal Communicator client (IMAP-related issues) (see also "Cisco Unified Personal Communicator client (IMAP-related issues)" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc

Table 2-2 Cisco Unity Connection Serviceability Macro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
ViewMail for Outlook (sending and receiving messages) (see also "ViewMail for Outlook (sending and receiving messages)" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
	ViewMail for Outlook	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection IMAP Server	diag_CuImapSvr_*.uc
		Connection Message Transfer Agent	diag_MTA_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
		Connection REST Service	diag_Tomcat_*.uc
		Connection Mailbox Sync	diag_CuMbxSync_*.uc
Cisco Unity Connection Serviceability Issues			
Cisco Unity Connection Serviceability	Connection Serviceability Web Service	Connection Tomcat Application	diag_Tomcat_*.uc
Conversation Issues			
Conversations	Conversation Traces	Connection Conversation Manager	diag_CuCsMgr_*.uc
Message Issues			
Dispatch messages (see also "Dispatch messages" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
IMAP messages (see also "IMAP messages" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
Message delivery and retrieval (see also "Message delivery and retrieval" in Table 2-1)	Message Tracking Traces	Connection Message Transfer Agent	diag_MTA_*.uc
		Connection System Agent	diag_CuSysAgent_*.uc
		Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Tomcat Application	diag_Tomcat_*.uc
		Connection IMAP Server	diag_CuImapSvr_*.uc
NDRs (see also "NDRs" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
Notifications not sent (see also "Notifications not sent" in Table 2-1)	Traces for Other Notification Problems (expand the macro trace to select SIP or SCCP)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc

Table 2-2 Cisco Unity Connection Serviceability Macro Traces for Selected Problems (continued)

Problem Area	Traces to Set	RTMT Service to Select	Trace Log Filename
Single inbox message synchronization	Single Inbox Traces	Connection Mailbox Sync	diag_CuMbxSync_*.uc
MWI Issues			
MWIs	Traces for MWI problems (expand the macro trace to select SIP or SCCP)	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
Networking Issues			
Intrasite Networking replication (see also "Intrasite Networking replication" in Table 2-1)	Digital Networking	Connection Digital Networking Replication Agent	diag_CuReplicator_*.uc
VPIM message delivery (see also "VPIM message delivery" in Table 2-1)	Call Flow Diagnostics	Connection Conversation Manager	diag_CuCsMgr_*.uc
Startup Issues			
Connection startup fails	Unity Startup	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Notifier	diag_CuNotifier_*.uc
Text to Speech Issues			
Text to Speech	Call Control (Miu) Traces (expand the macro trace to select SIP or SCCP)	Connection Conversation Manager	diag_CuCsMgr_*.uc
	Media (Wave) Traces	Connection Conversation Manager	diag_CuCsMgr_*.uc
		Connection Mixer	diag_CuMixer_*.uc
	Text to Speech (TTS) Traces	Connection Conversation Manager	diag_CuCsMgr_*.uc

Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems

When you use Cisco Unity Connection Serviceability micro traces or macro traces to troubleshoot problems in Cisco Unity Connection, you must first enable the applicable traces in Cisco Unity Connection Serviceability. Then you can use the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to collect and view the logs that are generated by the traces.

Do the applicable procedure:

- To Enable Cisco Unity Connection Serviceability Micro Traces and View Trace Logs, page 2-10
- To Enable Cisco Unity Connection Serviceability Macro Traces and View Trace Logs, page 2-10

To Enable Cisco Unity Connection Serviceability Micro Traces and View Trace Logs

Step 1 In Cisco Unity Connection Serviceability, on the Trace menu, select **Micro Traces**.

Step 2 On the Micro Traces page, in the Server field, select the name of the Connection server and select **Go**.

Step 3 In the Micro Trace field, select the micro trace that you want to set and select **Go**.

Step 4 Under Micro Traces, check the check boxes for the micro-trace levels that you want to set and select **Save**.

Step 5 Reproduce the problem.

Step 6 To collect the trace log files, launch the Real-Time Monitoring Tool (RTMT). For detailed instructions, see the "Working with Trace and Log Central" chapter of the applicable *Cisco Unified Real-Time Monitoring Tool Administration Guide*, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

You can access the trace log files by using the command line interface (CLI). For information, see the applicable *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 7 In RTMT, on the System menu, select **Tools > Trace > Trace & Log Central**.

Step 8 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

Step 9 In the Select CUC Services/Application tab, check the check boxes for the applicable services and select **Next**.

Step 10 In the Select System Services/Applications tab, select **Next**.

Step 11 In the Collection Time group box, specify the time range for which you want to collect traces.

Step 12 In the Download File option group box, specify the options you want for downloading traces.

Step 13 Select **Finish**.

Step 14 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.

Step 15 In Cisco Unity Connection Serviceability, disable the traces that you enabled in Step 3 and Step 4, then select **Save**.

To Enable Cisco Unity Connection Serviceability Macro Traces and View Trace Logs

Step 1 In Cisco Unity Connection Serviceability, on the Trace menu, select **Macro Traces**.

Step 2 On the Macro Traces page, in the Server field, select the name of the Connection server and select **Go**.

Step 3 Check the check box of the macro trace that you want to enable.

Step 4 Expand the macro trace, and check the check box for the levels that you want to enable.

Step 5 Select **Save**.

Step 6 Reproduce the problem.

Step 7 To collect the trace log files, launch the Real-Time Monitoring Tool (RTMT). For detailed instructions, see the "Working with Trace and Log Central" chapter of the applicable *Cisco Unified Real-Time Monitoring Tool Administration Guide*, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

You can access the trace log files by using the command line interface (CLI). For information, see the applicable *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 8 In RTMT, on the System menu, select **Tools > Trace > Trace & Log Central**.

Step 9 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

Step 10 In the Select CUC Services/Application tab, check the check boxes for the applicable services and select **Next**.

Step 11 In the Select System Services/Applications tab, select **Next**.

Step 12 In the Collection Time group box, specify the time range for which you want to collect traces.

Step 13 In the Download File option group box, specify the options you want for downloading traces.

Step 14 Select **Finish**.

Step 15 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.

Step 16 In Cisco Unity Connection Serviceability, disable the traces that you enabled in Step 3 through Step 5, then select **Save**.

For additional information on using Cisco Unity Connection Serviceability micro traces and macro traces, see the "Using Traces" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

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

For information on the CLI, see the applicable *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Traces in Cisco Unified Serviceability in Cisco Unity Connection 9.x

See the following sections:

Cisco Unified Serviceability Traces for Selected Problems

You can use Cisco Unified Serviceability traces to troubleshoot certain problems. After the traces are enabled, you can access the trace log files by using the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

Table 2-3 lists the information for Cisco Unified Serviceability traces that you need for troubleshooting selected problems and for viewing the trace logs. (For detailed information on using Cisco Unified Serviceability traces, see the "Trace" chapter of the applicable *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.)

Note Enabling Cisco Unified Serviceability traces decreases system performance. Enable traces only for troubleshooting purposes.

Table 2-3 Cisco Unified Serviceability Traces for Selected Problems

Problem Area	Traces to Set	RTMT Service to Select
Backing up and restoring	Cisco DRF Local Cisco DRF Master	Cisco DRF Local Cisco DRF Master
LDAP synchronization	Cisco DirSync	Cisco DirSync
Web application sign-in	Cisco CCMRealm Web Service	Cisco CallManager Realm

Using Cisco Unified Serviceability Traces to Troubleshoot Problems

When you use Cisco Unified Serviceability traces to troubleshoot problems in Cisco Unity Connection, you must first enable the applicable traces in Cisco Unified Serviceability. Then you can use the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to collect and view the logs that are generated by the traces.

Do the following procedure.

To Enable Cisco Unified Serviceability Traces and View Trace Logs

Step 1 In Cisco Unified Serviceability, on the Trace menu, select **Troubleshooting Trace Settings**.

Step 2 On the Troubleshooting Trace Settings page, under Directory Services, check the check box for the trace that you want to enable and select **Save**.

Step 3 Reproduce the problem.

Step 4 To collect the trace log files, launch the Real-Time Monitoring Tool (RTMT). For detailed instructions, see the "Working with Trace and Log Central" chapter of the applicable *Cisco Unified Real-Time Monitoring Tool Administration Guide*, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

You can access the trace log files by using the command line interface (CLI). For information, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 5 In RTMT, on the System menu, select **Tools > Trace > Trace & Log Central**.

Step 6 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

Step 7 In the Select CUC Services/Application tab, select **Next**.

Step 8 In the Select System Services/Applications tab, check the check boxes for the applicable service and select **Next**.

Step 9 In the Collection Time group box, specify the time range for which you want to collect traces.

Step 10 In the Download File option group box, specify the options you want for downloading traces.

Step 11 Select **Finish**.

Step 12 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.

Step 13 In Cisco Unity Connection Serviceability, disable the traces that you enabled in Step 2, and select **Save**.

For additional information on Cisco Unified Serviceability traces, see the "Trace" chapter of the applicable *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

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

For information on the CLI, see the applicable *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

CHAPTER 3

Troubleshooting Utilities Used in Cisco Unity Connection 9.x

This chapter provides brief descriptions of and procedures for accessing a selection of tools and utilities that can be used in troubleshooting Cisco Unity Connection.

See the following sections:

Cisco Unity Connection 9.x Grammar Statistics Tool

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

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

By default, Connection recompiles grammars when administrators add named objects or change object names on the system (unless a bulk operation is in progress, in which case Connection waits ten minutes for the operation to complete before recompiling the grammars), or when there are more than five changes requested in the space of a minute. If the grammars have grown to the point where the name grammar recompilation process is affecting the performance of your Connection server during busy periods, you can modify the default Voice Recognition Update Schedule (under System Settings >

Schedules in Cisco Unity Connection Administration) to limit the times and days when the Connection voice-recognition transport utility can automatically rebuild the voice-recognition name grammars. By default, all days and times are active for this schedule; if you modify the schedule but want to override the schedule while it is inactive and force an immediate recompilation of all grammars, or if you want to force recompilation during the ten minute wait period after a bulk operation has been initiated, you can select the Rebuild Grammars button on the Grammar Statistics tool.

Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x

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

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

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

For more information, see the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

Cisco Unity Connection 9.x Task Management Tool

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

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

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

To Access the Task Management Tool

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

Step 2 Select **Task Management**.

Cisco Voice Technology Group Subscription Tool in Cisco Unity Connection 9.x

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

Real-Time Monitoring Tool in Cisco Unity Connection 9.x

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

RTMT allows you to perform the following tasks:

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

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

Cisco Unified Serviceability in Cisco Unity Connection 9.x

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

- Saving alarms and events for troubleshooting and providing alarm message definitions.
- Saving trace information to various log files for troubleshooting.
- Providing feature services that you can turn on, turn off, and view through the Service Activation window.

- Providing an interface for starting and stopping feature and network services.
- Generating and archiving daily reports; for example, alert summary or server statistic reports.
- Monitoring the number of threads and processes in the system; uses cache to enhance the performance.

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

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

Remote Database Administration Tools in Cisco Unity Connection 9.x

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

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

For details on enabling remote database access, see the "Enabling Database Access for Remote Administration Tools" section in the "Administrative Tools in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Cisco Utilities Database Link for Informix (CUDLI) in Cisco Unity Connection 9.x

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

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

Remote Port Status Monitor in Cisco Unity Connection 9.x

The Remote Port Status Monitor (rPSM) provides a real-time view of the activity of each voice messaging port on Cisco Unity Connection to assist in troubleshooting conversation flow and other problems.

Download the tool and view training videos and Help at http://www.ciscounitytools.com/Applications/CxN/PortStatusMonitorCUC7x/PortStatusMonitorCUC7x.html.

Application Audit Logging in Cisco Unity Connection

Application audit logging reports configuration and administrative changes for Cisco Unity Connection Administration, Cisco Personal Communications Assistant, Cisco Unity Connection Serviceability, Cisco Unified Serviceability, Real-Time Monitoring Tool (RTMT), and the command-line interface (CLI). It also reports user authentication events for Connection clients that use the Representational State Transfer (REST) APIs, and reports API calls for clients that use the Cisco Unity Connection Provisioning Interface (CUPI) or the Diagnostic Portal API (used by Analysis Manager in RTMT).

Application audit logging is enabled by default. Users with the Audit Administrator role can configure auditing on the Tools > Audit Log Configuration page in Cisco Unified Serviceability. (By default, the application administration account that is created during installation is assigned the Audit Administrator role.) For Cisco Unified Communications Manager Business Edition, the Audit Log Configuration page settings also control auditing for Cisco Unified Communications Manager components.

To access the audit logs, users with the Audit Administrator role can use the Real-Time Monitoring Tool. In Trace and Log Central, go to System > Audit Logs > Nodes. After you select the node, another window displays System > Cisco Audit Logs. The application audit logs are stored in the AuditApp folder. In a Connection cluster, the publisher and subscriber each have separate application audit logs which you can reach by selecting the appropriate node.

Database and operating system audit logging are also available in Connection, although they are disabled by default. For more information on audit logging, see the "Configuring the Audit Log" chapter of the *Cisco Unified Serviceability Administration Guide*, *Release 9.0(1)*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html .

CHAPTER 4

Troubleshooting Reports in Cisco Unity Connection 9.x

When no data appears in the reports that you generate, use the following task list to determine the cause and to resolve the problem.

Task List for Troubleshooting Data in Reports

1. Confirm that the Connection Reports Data Harvester service is running. See the "Confirming That the Cisco Unity Connection 9.x Reports Data Harvester Service Is Running" section on page 4-1.
2. Adjust the report data collection cycle. See the "Adjusting the Report Data Collection Cycle in Cisco Unity Connection 9.x" section on page 4-2.
3. Use traces to troubleshoot reports. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

For information about the available reports and how to generate reports, see the "Using Reports" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

Confirming That the Cisco Unity Connection 9.x Reports Data Harvester Service Is Running

To Confirm That the Connection Reports Data Harvester Service Is Running

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 On the Control Center – Feature Services page, under Optional Services, locate the **Connection Reports Data Harvester** service.

Step 3 Confirm that the activate status for the Connection Reports Data Harvester service is **Activated**. If the activate status is Deactivated, select **Activate**.

Step 4 Confirm that the service status for the Connection Reports Data Harvester service is **Started**. If the service status is Stopped, select **Start**.

Step 5 Confirm that the running time for the Connection Reports Data Harvester service is greater than 00:00:00. If the running time is 00:00:00, turn off the Connection Reports Data Harvester service, then repeat Step 3 and Step 4.

Adjusting the Report Data Collection Cycle in Cisco Unity Connection 9.x

If the value of the Data Collection Cycle field is too high, the data may not have been collected yet for the report because the time between each cycle of collecting data is too long. Do the following procedure to correct the value.

To Adjust the Report Data Collection Cycle

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Reports**.

Step 2 On the Report Configuration page, in the Minutes Between Data Collection Cycles field, enter the time (in minutes) that you want between each cycle of collecting data for the reports. The default is 30 minutes.

Step 3 Select **Save**.

CHAPTER 5

Troubleshooting Fax in Cisco Unity Connection 9.x

See the following sections:

Problems with Fax Delivery to Users in Cisco Unity Connection 9.x

When faxes are not delivered to users, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Fax Delivery to Users

1. Determine whether the fax is being sent by enabling the MTA micro trace (all levels). For detailed instructions on enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
2. If the trace logs show that the fax was sent, investigate how the SMTP server handles faxes by enabling the SMTP micro trace (all levels). For detailed instructions on enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
3. Confirm that the SMTP server configuration lists the IP address of the Cisco Fax Server and allows a connection. See the "Confirming That the SMTP Server Configuration Is Correct" section on page 5-2.
4. Check for the fax in the POP3 mailbox by connecting an email client to the POP3 mailbox.

   Note that the email client must be configured to leave messages in the POP3 mailbox.
5. In the RightFax Email Gateway, confirm that the POP3 mailbox name and password are correct. See the "Confirming That the POP3 Mailbox Name and Password Are Correct" section on page 5-2.
6. On the network, confirm that the account for the POP3 mailbox is set to never expire the password. An expired password prevents faxes from being routed.

7. Confirm that faxes are delivered to Cisco Unity Connection. See the "Confirming That a Fax Is Delivered to Cisco Unity Connection" section on page 5-2.

Confirming That the SMTP Server Configuration Is Correct

To Confirm That the SMTP Server Configuration Is Correct

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **SMTP Configuration > Server**.

Step 2 On the SMTP Server Configuration page, on the Edit menu, select **Search IP Address Access List**.

Step 3 On the Search IP Address Access List page, confirm that the IP address of the Cisco Fax Server appears in the list. If not, select **Add New** to add the IP address.

Step 4 Check the **Allow Connection** check box for the IP address of the Cisco Fax Server, if it is not already checked.

Step 5 Select **Save**.

Confirming That the POP3 Mailbox Name and Password Are Correct

To Confirm That the POP3 Mailbox Name and Password Are Correct

Step 1 On the Windows Start menu, select **Control Panel > RightFax Email Gateway**.

Step 2 In the Email Configuration window, select the **General** tab.

Step 3 In the POP3 Mailbox Name field, confirm that the entry matches the SMTP address for the Cisco Fax Server on the System Settings > Fax Server > Edit Fax Server Configuration page in Cisco Unity Connection Administration.

Step 4 In the Mailbox Password field, confirm that the password is correct.

Step 5 In the Email Deliver Direction field, confirm that **Both** is selected.

Step 6 Select **OK**.

Confirming That a Fax Is Delivered to Cisco Unity Connection

To Confirm That a Fax Is Delivered to Cisco Unity Connection

Step 1 On the Windows Start menu, select **All Programs > RightFax FaxUtil**.

Step 2 In the RightFax FaxUtil window, in the left pane, select the user who will send the test fax.

Step 3 On the Fax menu, select **New**.

Step 4 In the Fax Information dialog box, select the **Main** tab.

Step 5 Under the Name field, select the drop-down arrow and select **Email Address**.

Step 6 In the Email Address field, enter the email address of the user who has the fax delivery problem.

Step 7 Select **Save**.

Step 8 In the right pane, note the status of the test fax as it is being sent.

Note To refresh the status display of the fax progress, press **F5**.

Problems with Fax Delivery to a Fax Machine in Cisco Unity Connection 9.x

When faxes are not delivered to a fax machine, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Fax Delivery to a Fax Machine

1. Determine the status of the fax that was sent to a fax machine. See the "Determining the Status of the Fax That Was Sent to a Fax Machine" section on page 5-3.
2. Confirm that the fax is in the POP3 mailbox by connecting an email client to the POP3 mailbox.

   Note that the email client must be configured to leave messages in the POP3 mailbox.
3. In the RightFax Email Gateway, confirm that the POP3 mailbox name and password are correct. See the "Confirming That the POP3 Mailbox Name and Password Are Correct" section on page 5-4.
4. On the network, confirm that the account for the POP3 mailbox is set to never expire the password. An expired password prevents faxes from being routed.
5. Confirm that the SMTP server configuration lists the IP address of the Cisco Fax Server and allows a connection. See the "Confirming That the SMTP Server Configuration Is Correct" section on page 5-4.
6. Troubleshoot how the SMTP server handles faxes by enabling the SMTP micro trace (all levels). For detailed instructions on enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
7. If the trace logs show that the SMTP message was not sent, investigate how the fax is sent by enabling the MTA micro trace (all levels). For detailed instructions on enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
8. Confirm that the file extension of the file that the user attempted to fax is included in the list of faxable file types. See the "Confirming That the Faxable File Types List Is Correct" section on page 5-4.

Determining the Status of the Fax That Was Sent to a Fax Machine

To Confirm That a Fax Is Delivered to the Cisco Fax Server

Step 1 On the Windows Start menu, select **All Programs > RightFax FaxUtil**.

Step 2 In the RightFax FaxUtil window, in the left pane, select the user who sent the fax to the fax machine, then select **All**.

Step 3 In the right pane, note the status of the fax and any problems that are reported.

Confirming That the POP3 Mailbox Name and Password Are Correct

To Confirm That the POP3 Mailbox Name and Password Are Correct

Step 1 On the Windows Start menu, select **Control Panel > RightFax Email Gateway**.

Step 2 In the Email Configuration window, select the **General** tab.

Step 3 In the POP3 Mailbox Name field, confirm that the entry matches the SMTP address for the Cisco Fax Server on the System Settings > Fax Server > Edit Fax Server Configuration page in Cisco Unity Connection Administration.

Step 4 In the Mailbox Password field, confirm that the password is correct.

Step 5 In the Email Deliver Direction field, confirm that **Both** is selected.

Step 6 Select **OK**.

Confirming That the SMTP Server Configuration Is Correct

To Confirm That the SMTP Server Configuration Is Correct

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **SMTP Configuration > Server**.

Step 2 On the SMTP Server Configuration page, on the Edit menu, select **Search IP Address Access List**.

Step 3 On the Search IP Address Access List page, confirm that the IP address of the Cisco Fax Server appears in the list. If not, select **Add New** to add the IP address.

Step 4 Check the **Allow Connection** check box for the IP address of the Cisco Fax Server, if it is not already checked.

Step 5 Select **Save**.

Confirming That the Faxable File Types List Is Correct

To Confirm That the Faxable File Types List Is Correct

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Fax**.

Step 2 On the Fax Configuration page, in the Faxable File Types field, note the file extensions that are listed.

Step 3 If the file extension of the file that the user attempted to fax is not in the list, enter a comma followed by the file extension and select **Save**.

Problems with Fax Notifications in Cisco Unity Connection 9.x

Confirm that fax notification from Cisco Unity Connection is enabled for the user. Do the following procedure.

To Confirm That Fax Notification Is Enabled for the User

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

Step 2 On the Search Users page, select the alias of the user.

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

Step 3 On the Edit menu, select **Notification Devices**.

Step 4 On the Notification Devices page, select the name of the applicable notification device.

Step 5 On the Edit Notification Device page, under Notification Rule Events, check the **Fax Messages** check box.

Step 6 Select **Save**.

Problems with Fax Receipts in Cisco Unity Connection 9.x

See the following sections, as applicable:

- Fax Receipts Are Not Delivered, page 5-5
- The User Mailbox Is Filled with Fax Notifications, page 5-7

Fax Receipts Are Not Delivered

Confirm that the prefixes for delivery receipts and nondelivery receipts (NDRs) are correct. Do the following procedures.

To Verify Prefixes for Delivery Receipts and Nondelivery Receipts on the Cisco Fax Server

Step 1 On the Windows Start menu, select **Control Panel > RightFax Enterprise Fax Manager**.

Step 2 In the Email Configuration window, select the **General** tab.

Step 3 In the left pane of the RightFax Enterprise Fax Manager window, select the name of the Cisco Fax Server.

Step 4 In the right pane, under Service Name, scroll down to **RightFax eTransport Module**.

Step 5 Right-click **RightFax eTransport Module** and select **Configure Services**.

Step 6 Select the **Custom Messages** tab.

Step 7 In the applicable fields, verify the fax failure prefix at the beginning of the text (the default fax failure prefix is [Fax Failure]). We recommend that the fax failure prefix appear at the beginning of the following fields:

- Imaging Error
- Bad Form Type
- Bad Fax Phone Number
- Too Many Retries
- Sending Error
- Incomplete Fax
- Invalid Billing Code
- Fax Needs Approval
- Fax Number Blocked
- Human Answered Fax
- Fax Block by Do Not Dial

When the text at the beginning of the field matches the value for the Subject Prefix for Notification of a Failed Fax field on the System Settings > Advanced > Fax page of Cisco Unity Connection Administration, Connection notifies the user of the failed fax.

Step 8 In the Successful Send field, verify the fax success prefix at the beginning of the text (the default fax success prefix is [Fax Success]).

When the text at the beginning of the field matches the value for the Subject Prefix for Notification of a Successful Fax field on the System Settings > Advanced > Fax page of Connection Administration, Connection notifies the user of the successful fax.

Step 9 Select **OK**.

To Verify Prefixes for Delivery Receipts and Nondelivery Receipts on Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Fax**.

Step 2 On the Fax Configuration page, in the Subject Prefix for Notification of a Successful Fax field, confirm that the setting matches the prefix for the Successful Send field that is described in Step 8 of the "To Verify Prefixes for Delivery Receipts and Nondelivery Receipts on the Cisco Fax Server" procedure on page 5-5.

Step 3 In the Subject Prefix for Notification of a Failed Fax field, confirm that the setting matches the prefix for the fields that are described in Step 7 of the "To Verify Prefixes for Delivery Receipts and Nondelivery Receipts on the Cisco Fax Server" procedure on page 5-5.

Step 4 Select **Save**.

The User Mailbox Is Filled with Fax Notifications

If the user mailbox is filled with fax notifications, do the following procedure.

To Disable Fax Notifications

Step 1 In the RightFax Enterprise Fax Manager window, in the right pane, expand **Users**, right-click the user for whom you want to disable fax notifications, and select **Edit**.

Step 2 In the User Edit dialog box, select the **Notifications** tab.

Step 3 Under Notification About Received Faxes, uncheck the **When Initially Received** check box.

Step 4 Select **OK**.

Step 5 Repeat Step 1 through Step 4 for all remaining users for whom you want to disable fax notifications.

Step 6 Close the RightFax Enterprise Fax Manager window.

Problems with Printing Faxes in Cisco Unity Connection 9.x

When you send a fax to a fax machine for printing but portions of the document are not printed, do the following:

- Use the MTA micro trace to determine which files are not rendered into the fax. Then note the file types. For instructions for enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
- Confirm that the faxable file types include the file types that you sent to the fax machine for printing. See the "Confirming That the Faxable File Types List Is Correct" section on page 5-7.

Confirming That the Faxable File Types List Is Correct

To Confirm That the Faxable File Types List Is Correct

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Fax**.

Step 2 On the Fax Configuration page, in the Faxable File Types field, note the file extensions that are listed.

Step 3 If the file extension of the file that the user attempted to fax is not in the list, enter a comma followed by the file extension and select **Save**.

CHAPTER 6

Troubleshooting External Services (External Message Store, Calendar Integrations, Calendar Information for PCTRs) in Cisco Unity Connection 9.0

See the following sections:

For information on troubleshooting unified messaging in Cisco Unity Connection , see the "Troubleshooting Microsoft Office 365 for Unified Messaging in Cisco Unity Connection" chapter.

Troubleshooting Access to Emails in an External Message Store in Cisco Unity Connection 9.0

See the following sections for information on troubleshooting problems with accessing emails in an external message store:

User on the Phone Hears "Invalid Selection" After Pressing 7

When a user has signed in by phone, presses 7 on the main menu, and is told that the selection is invalid, the external service account for the user is not enabled for access to email in the external message store. Do the following procedure.

To Enable User Access to Email in an External Message Store

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

Step 2 On the Search Users page, select the alias of the user.

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

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select the name of the external service that connects to the external message store.

Step 5 On the Edit External Service Account page, check the **User Access to Email in Third-Party Message Store** check box and select **Save**.

User on the Phone Hears "Your Messages Are Not Available" After Pressing 7

When a user has signed in by phone, presses 7 on the main menu, and is told that messages are not available, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a "Your Messages Are Not Available" Message

1. Test the external service that enables access to email in the external message store, and correct any errors that are reported. See the "Testing the External Service That Enables Access to Email in an External Message Store" section on page 6-4.
2. Test the external service account of the user who is enabled to access email in the external message store, and correct any errors that are reported. See the "Testing the External Service Account for Users Enabled to Access Email in an External Message Store" section on page 6-4.
3. In Cisco Unity Connection Administration, on the Class of Service > Edit Class of Service page for the class of service to which the user is assigned, confirm that the Allow Access to Email in Third-Party Message Stores check box is checked.
4. In Connection Administration, on the Users > Edit External Service Accounts page for the user, confirm that the Access to Email in Third-Party Store check box is checked. See the "Enabling User Access to Email in an External Message Store" section on page 6-4.
5. In Connection Administration, on the Users > Edit External Service Accounts page for the user, confirm that the User ID field entry matches the Exchange login alias of the user. If the Login Type field is set to Use Connection Alias, the user Exchange login alias must match the Connection user alias.
6. On the Exchange server, confirm that the Microsoft Exchange IMAP4 service is running.

7. Ping the server to which the external service connects by using the value in the Server field on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page in Connection Administration. If the ping fails, the network connection is not functional. You must restore the net work connection.
8. Confirm that the Exchange server is set up to support basic authentication for IMAP4.
9. If Exchange requires SSL, Connection may be configured for an open connection. In Connection Administration, on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page, confirm that Security Transport Type field is set to SSL.

   You can manually check whether the Exchange server accepts open IMAP connections by entering the following commands at the command prompt:

   telnet <Exchange server IP address> 143

   01 login <NT domain>/<Connection service account>/<Exchange user> <password>
   02 select inbox
10. If Exchange is not enabled for SSL, Connection may be configured for a secure connection, and you must install a server certificate on the Exchange server to enable SSL. Otherwise, in Connection Administration, on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page, set the Security Transport Type field to None.
11. If the external service is configured for SSL and the Validate Server Certificate check box is checked, determine whether certificate validation is causing the problem. Do the following sub-tasks:
    a. In Connection Administration, on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page, uncheck the **Validate Server Certificate** check box and select **Save**.
    b. On a phone, sign in as the user who experiences the problem and press **7** at the main menu.
    c. If the user is able to access email on the external message store, confirm that the CN field of the Exchange certificate subject line matches the value of the Server field on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page in Connection Administration.
    d. Confirm that the public root certificate of the Certificate Authority (CA) that issued the Exchange server certificate is installed on Connection as a trusted certificate, that it is self-signed, and that it has not expired.
    e. In Connection Administration, on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page, check the **Validate Server Certificate** check box and select **Save**.
12. In Connection Administration, on the System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page, confirm that the values of the Alias and Password fields are correct.

    Note You must enter the value in the Alias field in the NT domain qualified format (for example, companydomain\jdoe).
13. Confirm that the service account on Exchange that the external service uses has the Administer Information Store, Receive As, and Send As permissions allowed.
14. If the Exchange server is slow to respond to IMAP requests so that Connection times out, in Connection Administration, on the System Settings > Advanced > External Services page, set the Maximum External Service Response Time field to a value greater than 4.

Note Increasing the value of the Maximum External Service Response Time may result in delays when accessing email in an external message store.

Testing the External Service That Enables Access to Email in an External Message Store

Do the following procedure.

To Test the External Service That Enables Access to Email in an External Message Store

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

Step 2 On the Search External Services page, select the name of the applicable external service.

Step 3 On the Edit External Service page, select **Test**.

Step 4 In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

Step 5 Repeat Step 3 and Step 4 until the test succeeds.

Testing the External Service Account for Users Enabled to Access Email in an External Message Store

Do the following procedure.

To Test the External Service Account for Users Enabled to Access Email in an External Message Store

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

Step 2 On the Search Users page, select the alias of the user.

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

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select the name of the applicable external service account.

Step 5 Select **Test**.

Step 6 In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

Step 7 Repeat Step 5 and Step 6 until the test succeeds.

Enabling User Access to Email in an External Message Store

Do the following procedure.

To Enable User Access to EMail in an External Message Store

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

Step 2 On the Search Users page, select the alias of the user.

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

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select the name of the external service that connects to the external message store.

Step 5 On the Edit External Service Account page, check the **User Access to Email in Third-Party Message Store** check box and select **Save**.

Users Cannot Access All Options While Listening to Email

While listening to email on the phone, users have the same options that are allowed with voice messages, except for the following, which are not allowed for email:

- Reply (includes live reply and reply to all)
- Forward
- Permanently delete individual emails

  Users can permanently delete all soft-deleted email at once through the same conversation that they would use to permanently delete all soft-deleted voice messages.

Users Hear Gibberish at the End or Beginning of an Email

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

Email Deleted by Phone Is Still in the Inbox Folder

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

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

Short Delays or No Access While Listening to Email

While listening to email (external messages) on the phone, a user may experience up to a four-second delay, or a user may be told that email could not be read. This behavior may be intermittent.

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

Microsoft Exchange can respond slowly for a number of reasons, but the most common reason is that the user has a large number of messages in his or her Inbox folder (for example, more than 1,000 messages). One solution may be to have the user delete messages or reorganize the email folders to reduce the number of messages in the Inbox.

Another solution is to increase the amount of time Connection waits to access the external message store before timing out. In Cisco Unity Connection Administration, expand System Settings > Advanced > External Services and change the setting for Maximum External Service Response Time from the default setting of 4 seconds to 6 or 10 seconds. Increasing the timeout value gives Exchange more time to respond to IMAP requests and successfully retrieve messages, but callers may experience long pauses while waiting for the system to respond.

Using Traces to Troubleshoot Access to Emails in an External Message Store (All Versions of Exchange)

You can use traces to troubleshoot access to emails in an external message store. For detailed instructions, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

Troubleshooting Calendar Integrations in Cisco Unity Connection 9.0

See the following sections for information on troubleshooting problems with calendar integrations:

How External User Accounts Are Used for Calendar Integrations

The following configuration principles apply to external service accounts that are used for calendar integrations:

- A user can have only one external service account for which the User Access to Calendar and Personal Contacts check box is checked.
- A user can have multiple external service accounts for which the MeetingPlace Scheduling and Joining check box is checked.
- If there are multiple external service accounts for which the MeetingPlace Scheduling and Joining check box is checked, a user must have only one external service account for which the Primary Meeting Service check box is checked.

Each user can access calendar information from only one external service account. If the calendar-enabled external service account connects to an Exchange server, the user has access to events only from the Exchange calendar. Similarly, if the calendar-enabled external service account connects to a Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express server, the user has access to events only from the Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express calendar.

The Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express server that is used to schedule reservationless meetings is designated by the external service account for which the Primary Meeting Service check box is checked.

For information on configuring a calendar integration between Cisco Unity Connection and Exchange 2003, see the "Creating Calendar and Contact Integrations in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Testing the Calendar Integration

Do the following procedure to test the calendar integration.

To Test the Calendar Integration

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

Step 2 On the Search Users page, select the alias of a user.

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

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select the name of the applicable external service account.

Step 5 Select **Test**.

Step 6 In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

Step 7 Repeat Step 5 and Step 6 until the test succeeds.

Test Fails the Last Check (Exchange 2003 Only)

When you select Test on the Edit External Service Account page to troubleshoot a calendar integration and all checks succeed except for the last check (which fails with the message "The system failed to perform a typical calendar operation"), use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting When the Test Fails the Last Check

1. On the Exchange server, confirm that SP1 or later is installed.
2. On the Exchange server, confirm that the user is enabled for Outlook Web Access (OWA).
3. In Cisco Unity Connection Administration, on the Users > Edit External Service Accounts page for the user, confirm that the entry in the Email Address field matches the primary SMTP address for the user.
4. On the Exchange server, confirm that the Microsoft Exchange Outlook Web Access service is available.

   You can manually check whether the Microsoft Exchange Outlook Web Access service is available by entering the following URL in a web browser:

   http://<servername>/exchange/<emailaddress>

   Note that the URL must begin with "https:" if SSL is selected in the Security Transport Type field on the System Settings > External Services > Edit External Service page. For <servername>, enter the value of the Server field on the System Settings > External Services > Edit External Service page to which the user external service account refers. For <emailaddress>, enter the value of the Email Address field on the Users > Edit External Service Account page for the user. When prompted to authenticate, enter the values of the Alias and Password fields on the System Settings > External Services > Edit External Service page.
5. In Cisco Unified Operating System Administration, on the Services > Ping Configuration page, confirm that Connection can ping the IP address or hostname of the Exchange server.
6. If the external service is configured for SSL and the Validate Server Certificate check box is checked, determine whether certificate validation is causing the problem by doing the following sub-tasks.
   a. In Connection Administration, on the System Settings > External Services > Edit External Services page, uncheck the **Validate Server Certificate** check box and select **Save**.
   b. On a phone, sign in as the user who experiences the problem and access calendar information.
   c. If the user is able to access calendar information, confirm that the public root certificate of the Certificate Authority (CA) that issued the Exchange server certificate is installed on Connection as a trusted certificate, that it is self-signed, and that it has not expired.
   d. In Connection Administration, on the System Settings > External Services > Edit External Services page, check the **Validate Server Certificate** check box and select **Save**.
7. In Connection Administration, on the System Settings > External Services > Edit External Services page, confirm that the values of the Alias and Password fields are correct.

   Note You must enter the value in the Alias field in the NT domain qualified format (for example, companydomain\jdoe).
8. Confirm that the service account on Exchange that the external service uses has the Administer Information Store, Receive As, and Send As permissions allowed.

9. If the Exchange server is slow to respond to calendar information requests so that Connection times out, in Connection Administration, on the System Settings > Advanced > External Services page, set the Maximum External Service Response Time field to a value greater than 4.

Note Increasing the value of the Maximum External Service Response Time may result in delays when accessing calendar information.

Test Succeeds, but the Calendar Integration Still Does Not Work (Exchange 2003 Only)

When you select Test on the Edit External Service Account page to troubleshoot a calendar integration and all checks succeed but the calendar integration still does not work, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a Calender Integration When the Test Succeeds

1. In Cisco Unity Connection Administration, on the Users > Edit External Service Accounts page for the user, confirm that the fully qualified DNS name (FQDN) of the Exchange server is resolvable via DNS.

   Even if the Users > Edit External Service Accounts page for the user is configured with the IP address of the Exchange server, calendar information from the Exchange server is provided with URLs that contain the FQDN of the server. Connection uses these URLs, which must be resolved by a DNS server so that the user can access calendar information.

2. If the Exchange server is slow to respond to calendar information requests so that Connection times out, in Connection Administration, on the System Settings > Advanced > External Services page, set the Maximum External Service Response Time field to a value greater than 4.

   Note Increasing the value of the Maximum External Service Response Time may result in delays when accessing calendar information.

3. Confirm that the system clocks on the Connection and Exchange servers are both correct.
4. Confirm that the meetings appear on the Outlook calendar of the user.

   If Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express meetings are scheduled through the user web interface for these applications, the scheduled meetings do not appear on the Outlook calendar of the user. If you configure the profile for Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express with an email type of “Exchange,” meeting requests appear on the Outlook calendar of the user.

Non-Published Meetings Do Not Appear in List of Meetings (Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express Only)

When Cisco Unity Connection has an calendar integration with Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express, all applicable published and non-published meetings are listed when the user accesses meeting information.

If non-published meetings are not listed in the list of meetings, the service account that Connection uses to access calendar information is not correctly configured. Do the applicable procedure to configure the service that Connection uses.

To Configure the Connection Service Account (Cisco Unified MeetingPlace Only)

Step 1 Sign in to the Cisco Unified MeetingPlace Administration Server as an administrator.

Step 2 Select **User Configuration > User Profiles**.

Step 3 Select the Connection service account.

Step 4 In the Type of User field, select **System Administrator**.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace.

To Configure the Connection Service Account (Cisco Unified MeetingPlace Express Only)

Step 1 Sign in to Cisco Unified MeetingPlace Express and select **Administration**.

Step 2 Select **User Configuration > User Profile Management**.

Step 3 Select the Connection service account.

Step 4 In the Type of User field, select **API User**.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace Express.

Meetings Do Not Appear in List of Meetings

When meetings do not appear in the list of meetings, the cause may be the interval that Cisco Unity Connection waits to update calendar information. Do the following procedure.

To Change the Interval That Cisco Unity Connection Waits to Update Calendar Information

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **External Services**.

Step 2 On the External Services Configuration page, in the Normal Calendar Caching Poll Interval field, enter the length of time (in minutes) that Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner. A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.

Step 3 In the Short Calendar Caching Poll Interval field, enter the length of time (in minutes) that Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

This setting applies to users who have the Use Short Calendar Caching Poll Interval check box checked on their Edit User Basics page.

Step 4 Select **Save**.

Users Cannot Save New External Service Account with Access to Calendar

When you cannot create a new external service account on which the User Access to Calendar and Personal Contacts check box is checked, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting an External Service That Cannot Be Saved

1. In Cisco Unity Connection Administration, on the System Settings > External Services > Edit External Services page, confirm that on the external service that is referenced by the user external service account, the User Access to Calendar and Personal Contacts check box is checked.
2. In Connection Administration, on the Users > Edit External Service Accounts page for the user, confirm that the user does not have another external service account on which the User Access to Calendar and Personal Contacts check box is checked. A user can have only one external service account on which the User Access to Calendar and Personal Contacts check box is checked.

Using Traces to Troubleshoot a Calendar Integration

You can use traces to troubleshoot a calendar integration. For detailed instructions, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

Troubleshooting Access to Calendar Information When Using Personal Call Transfer Rules in Cisco Unity Connection 9.0

You can use traces to troubleshoot issues related to accessing calendar information when using personal call transfer rules. For detailed instructions, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

See also the "Troubleshooting Personal Call Transfer Rules in Cisco Unity Connection 9.x" chapter.

Troubleshooting the Test Button on Pages for External Services and External Service Accounts in Cisco Unity Connection 9.0

You can use traces to troubleshoot problems with the Test button (the external service diagnostic tool). This button is available on the following pages in Cisco Unity Connection Administration:

- System Settings > External Services > Email, Calendar, and Contacts > Edit External Services page
- Users > Users > Edit External Service Account page

For information on using traces to troubleshoot problems with the Test button, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

CHAPTER 7

Troubleshooting Unified Messaging in Cisco Unity Connection

See the following sections:

Troubleshooting Single Inbox in Cisco Unity Connection

Cisco Unity Connection must be configured with Dual Mode (IPv4/IPv6) for IPv6 communication with Microsoft Exchange 2007, 2010, and 2013. For more information see the chapter “Adding or Changing the IPv6 Addresses of Cisco Unity Connection ” at the following link http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrug051.html

For information on troubleshooting external services in Cisco Unity Connection 9.0, see the “Troubleshooting External Services (External Message Store, Calendar Integrations, Calendar Information for PCTRs) in Cisco Unity Connection 9.0” chapter.

See the following sections:

Date and Time on Messages in Cisco Unity Connection Do Not Match the Date and Time on Messages in Exchange 2003

In the following circumstances, the date and time that a Cisco Unity Connection message was received does not match the date and time on the same message that has been synchronized with Exchange 2003:

- A Connection user already has voice messages when the Connection administrator configures single inbox for the user. In Connection, the messages continue to have the date and time that they were received. In Exchange 2003, the messages have the date and time that they were synchronized with Exchange.
- A Connection administrator uses the Disaster Recovery System to restore voice messages, and the backup contains messages that do not exist in Exchange 2003 because the user deleted them from Exchange after the backup. Connection resynchronizes the voice message into Exchange. The date and time on the messages in Connection are the original date and time that the messages were received, but the date and time on the messages in Exchange is the date and time that they were synchronized with Exchange.
- Single inbox is configured, and connectivity between Connection and Exchange 2003 is interrupted and restored. In Connection, messages received during the interruption in connectivity have the date and time that they were received. In Exchange, the messages have the date and time that they were synchronized after connectivity is restored.

Message Relay Is Not Working or Is Not Working as Expected

If messages are not being relayed at all, confirm that you have specified the IP address for an SMTP smart host through which Connection relays SMTP messages. (If DNS is configured, you can also specify the fully qualified domain name of the smart host.) In Connection Administration, see the System Settings > SMTP Configuration > Smart Host page.

If messages are being relayed but not as you expect, settings are probably combining in ways you had not anticipated. For a summary of how message actions are relaying messages for a specific user, in Connection Administration, see the Message Actions page for that user.

If messages are disappearing, see the "Cisco Unity Connection Is Unable to Relay Messages" section on page 16-5.

Single Inbox Is Not Working for Anyone on a Connection Server

When single inbox is not working for any of the users on a Connection server (for example, Connection voice messages are not synchronized into Exchange or Microsoft Office 365, and messages sent from ViewMail for Outlook are not delivered), do the following tasks.

1. On the primary server, in Cisco Unity Connection Serviceability, go to **Tools > Service Management**, and confirm that the service status for the following services is Started:
   - Connection Mailbox Sync (in the Critical Services section)
   - Connection Jetty (in the Optional Services section)
2. If a firewall is configured between the Connection and Exchange servers or between Connection and Active Directory domain controllers, confirm that the necessary ports are opened. For more information, see the "IP Communications Required by Cisco Unity Connection 9.x" chapter in the *Security Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.

Single Inbox Is Not Working for Users Associated with a Unified Messaging Service

Exchange

When single inbox is not working (for example, Connection voice messages are not synchronized into Exchange, and messages sent from ViewMail for Outlook are not delivered), and when the problem is occurring only for the Connection users whose unified messaging accounts are associated with the same unified messaging service, do the following tasks.

Note When a cluster is configured, do the Connection-specific tasks only on the primary (active) server.

1. Confirm that the unified messaging service is enabled and that single inbox is enabled:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, confirm that the **Enabled** check box is checked.
   b. Confirm that the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box is checked.
2. Test the unified messaging service:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, select **Test**.
   b. Correct any problems that are listed on the Task Execution Results page.
3. Test one of the affected unified messaging accounts:
   a. In Connection Administration, on the **Users > Edit User Basics > Unified Messaging Accounts** page, select **Test**.
   b. Correct any problems that are listed on the Task Execution Results page. Among the problems that the Task Execution Results page may list are the following browser errors:

      401 error: Possible causes include an incorrect password for the unified messaging services account, an incorrect username, or an invalid format for the username. (If you use the domain\user format, do not use FQDN format for the domain name.) Another possible cause is that the value of the Web-Based Authentication Mode list does not match the authentication mode configured in Exchange. All values appear on the Edit Unified Messaging Service page.

      403 error: SSL is required in Exchange, but the public certificates from the certification authority (CA) that signed the certificates on the Exchange servers have not been uploaded to the Connection server.

      404 error: One possible cause is that the unified messaging service is configured to use the HTTPS protocol to communicate with Exchange servers, but SSL is not enabled in Exchange. Another possible cause is that you are using Exchange 2003 as the message store, but WebDav extensions have not been enabled.
4. In Cisco Unity Connection Serviceability, go to **Tools > Service Management**. In the Critical Services section, confirm that the service status for the Connection Mailbox Sync service is Started.
5. Check Active Directory settings on the unified messaging services account:
   – Confirm that the account is not locked.
   – Confirm that the password for the account has not expired.

6. Temporarily replace the unified messaging services account with the Active Directory account for a Connection user associated with this unified messaging service:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, in the Username and Password fields, replace the credentials for the unified messaging services account with the credentials for a Connection user associated with this unified messaging service.
   b. Send the user a Connection voice message, and determine whether the voice message synchronized to Exchange.

      If the message did not synchronize, switch the Username and Password fields back to the values for the unified messaging services account, then skip to Task 7.

      If the message did synchronize, the problem is probably with permissions on the unified messaging services account. Continue with Task 6.c.
   c. Switch the Username and Password fields back to the values for the unified messaging services account.
   d. Regrant permissions as documented in the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection " section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.
   e. Send the Connection user another voice message, and determine whether the voice message synchronized to Exchange.

      If the message did not synchronize, skip to Task 7.

      If the message did synchronize, test with some other users who are associated with the same unified messaging service to ensure that the problem is resolved.
7. If Exchange mailboxes for the users are all homed on the same Exchange server, confirm that the required services are running on the Exchange servers:
   - If the mailboxes are all homed on one Exchnage 2013, Exchange 2010 or Exchange 2007 server, confirm that the EWS virtual directory is running on that Exchange server.
   - If the mailboxes are all homed on one Exchange 2003 server, confirm on that Exchange server that the WebDav extensions are enabled in IIS and that the WebDav virtual directory (Exchange) is configured properly.

   f. Confirm that Exchange authentication and SSL settings are the same on all Exchange servers, and confirm that Connection settings match the Exchange settings. For more information, see the "Confirming Exchange Authentication and SSL Settings for Cisco Unity Connection " section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.
8. If you configured the unified messaging service to validate certificates for Exchange servers or for Active Directory domain controllers:
   - Confirm that the applicable certification authority certificates have been uploaded to the Connection server.
   - Confirm that the certification authority certificates have not expired.

g. For more information, see the "Uploading CA Public Certificates for Exchange and Active Directory Servers to the Cisco Unity Connection Server " section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

9. If all Connection users associated with this unified messaging service have mailboxes homed on the same Exchange server, and if you are using HTTPS as the web-based protocol, confirm that SSL is properly configured:
   a. Confirm that certification authority certificates have been uploaded to the Connection server.
   b. In Connection Administration, confirm that the Exchange server name specified in the unified messaging service exactly matches the common name in the SSL certificate for that Exchange server.
   c. Confirm that the SSL certificates have not expired.
10. Use Microsoft EWSEditor to try to access the Exchange mailbox of a Connection user by using the unified messaging services account. This allows you to determine whether the problem occurs even when Connection is not involved.

    EWSEditor software and documentation are available on the Microsoft website.
11. Confirm DNS settings:
    - Confirm that the Exchange server is reachable from Connection.
    - If you configured the unified messaging service to search for Exchange servers, confirm that the Connection server is configured to use DNS.
    - If you configured the unified messaging service to search for Exchange servers, confirm that the name of the Exchange server is resolvable by the DNS server that Connection is configured to use.
    - If you configured the unified messaging service to search for Exchange servers, confirm that the DNS server that Connection is using is configured with appropriate records for autodiscovery.

Microsoft Office 365

When single inbox is not working (for example, Connection voice messages are not synchronized into Office 365, and messages sent from ViewMail for Outlook are not delivered), and when the problem is occurring only for the Connection users whose unified messaging accounts are associated with the same unified messaging service, do the following tasks.

Note When a cluster is configured, do the Connection-specific tasks only on the primary (active) server.

1. Confirm that the unified messaging service is enabled and that single inbox is enabled:
   a. In Connection Administration, on the Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service page, confirm that the Enabled check box is checked.
   b. Confirm that the Synchronize Connection and Exchange Mailboxes (Single Inbox) check box is checked.
2. Test the unified messaging service:
   a. In Connection Administration, on the Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service page, select Test.

b. Correct any problems that are listed on the Task Execution Results page.

3. Test one of the affected unified messaging accounts:
   a. In Connection Administration, on the Users > Edit User Basics > Unified Messaging Accounts page, select Test.
   b. Correct any problems that are listed on the Task Execution Results page. Among the problems that the Task Execution Results page may list are the following browser errors:

      401 error: Possible causes include an incorrect password for the unified messaging services account, an incorrect username, or an invalid format for the username.

      403 error: SSL is required in Office 365, but the public certificates from the certification authority (CA) that signed the certificates on the Office 365 servers have not been uploaded to the Connection server.
4. In Cisco Unity Connection Serviceability, go to **Tools > Service Management**. In the Critical Services section, confirm that the service status for the Connection Mailbox Sync service is Started.
5. Check the Active Directory settings on the unified messaging services account:
   - Confirm that the account is not locked.
   - Confirm that the password for the account has not expired.
6. Temporarily replace the unified messaging services account with the Active Directory account for a Connection:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, in the Username and Password fields, replace the credentials for the unified messaging services account with the credentials for a Connection user associated with this unified messaging service.
   b. Send the user a Connection voice message, and determine whether the voice message synchronized to Office 365.

      If the message did not synchronize, switch the Username and Password fields back to the values for the unified messaging services account, then skip to Task 7.

      If the message did synchronize, the problem is probably with permissions on the unified messaging services account. Continue with Task 6.c.
   c. Switch the Username and Password fields back to the values for the unified messaging services account.
   d. Send the Connection user another voice message, and determine whether the voice message synchronized to Office 365.

      If the message did not synchronize, skip to Task 7.

      If the message did synchronize, test with some other users who are associated with the same unified messaging service to ensure that the problem is resolved.
7. Confirm that SSL settings are the same on all Office 365 servers, and confirm that Connection settings match the Office 365 settings.
8. Confirm that Office 365 servers, which Connection accesses have authentication mode set to **Basic** and web-based protocol set to **HTTPS**
9. If you configured the unified messaging service to validate certificates for Office 365 servers or for Active Directory domain controllers:
   - Confirm that the applicable certification authority certificates have been uploaded to the Connection server.

- Confirm that the certification authority certificates have not expired.

Single Inbox Is Not Working for a User or a Subset of Users

When single inbox is not working (for example, Connection voice messages are not synchronized into Exchange, and messages sent from ViewMail for Outlook are not delivered), and when the problem is occurring for one or more Connection users but not for all users associated with a unified messaging service, do the following tasks.

Note When a cluster is configured, do the Connection-specific tasks only on the primary (active) server.

1. In Connection Administration, on the Users > Unified Messaging Accounts page for the user, confirm that the user is associated with a unified messaging service on which single inbox is enabled.
2. If you created an Exchange 2010 mailbox for the unified messaging services account, and if Exchange mailboxes for the affected users were moved from one Exchange 2003 mailbox store to another, delete the Exchange 2010 mailbox. For more information, see the "Exchange 2010 Mailbox Can Be Deleted for the Unified Messaging Services Account" section in the "New and Changed Requirements and Support—Release 9.0(1)" section of *Release Notes for Cisco Unity Connection Release 9.0(1)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/release/notes/901cucrn.html.
3. In Connection Administration, on the Users > Unified Messaging Accounts page for the user, confirm that single inbox is enabled in one of the user's unified messaging accounts.
4. In Connection Administration, on the Users > Unified Messaging Accounts page for the user, confirm that Connection is configured to use the correct Exchange email address.
5. In Connection Administration, on the Users > SMTP Proxy Addresses page for the user, confirm that there is an SMTP proxy address that matches the user's Exchange mail address.
6. If the user's Exchange mailbox was not moved, skip to Task 8.

   If the user's Exchange mailbox was moved, and if the user is associated with a unified messaging service that specifies an Exchange server instead of allowing Connection to search for Exchange servers, determine whether Connection is able to automatically detect mailbox moves. See the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.
7. If the user's Exchange mailbox is homed on a new Exchange server, confirm that the unified messaging services account has the permissions necessary to access the server. For more information, see the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection " section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.
8. If single inbox is not working for all of the Connection users whose mailboxes are homed on the same Exchange server, confirm that the required services are running on the Exchange servers:

- If the mailboxes are all homed on an Exchange 2013, Exchange 2010 or Exchange 2007 server, confirm that the EWS service is running on that Exchange server.
- If the mailboxes are all homed on an Exchange 2003 server, confirm that the WebDav service is running on that Exchange server.

9. If single inbox is not working for all of the Connection users whose mailboxes are homed on the same Exchange server, and if you are using HTTPS as the web-based protocol, confirm that SSL is properly configured:
   - In Connection Administration, uncheck the Validate Certificates for Exchange Servers check box, and determine whether single inbox is now working.
   - Confirm that SSL certificates have been uploaded to the Connection server.
   - Confirm that the SSL certificates have not expired.

Single Inbox Synchronization from Exchange Is Delayed

If Connection synchronization to Exchange is working (for example, voice messages are synchronized to users' Exchange mailboxes) but synchronization from Exchange is delayed (for example, the message waiting indicator is not turned off immediately after the last Connection voice message is heard in ViewMail for Outlook), do the following tasks.

1. In Cisco Unity Connection Serviceability, go to **Tools > Service Management**, and confirm that the service status for the Connection Jetty service is Started. If not, activate and start the service, then test one of the affected users.
2. At a command line on the Exchange server, run the following command to telnet from the Exchange server to the Connection server (confirm that port 7080 is open in the firewall, if applicable):

   telnet <*IP address of the Connection server*> **7080**

   If no error message is returned, the Exchange server was able to connect to the Connection server. If an error message is returned:
   - In Cisco Unity Connection Serviceability, confirm that the Connection Jetty service is running.
   - Troubleshoot the problem as you would any network issue.

   Press **Ctrl-K** to exit from Telnet.
3. In Cisco Unity Connection Administration, display the unified messaging account for one of the affected users, and select **Reset**.

   If synchronization from Exchange to Connection starts working for the affected user, in Connection Administration, display the unified messaging service associated with the affected user (Unified Messaging > Unified Messaging Services), and select **Reset**.

Caution While Connection is resynchronizing data with Exchange, synchronization will be delayed for all of the users associated with the unified messaging service.

Single Inbox Synchronization from Exchange Is Failed

If synchronization from Connection to Exchange fails for set of users and the unified messaging account Reset button press is not resolving the problem, do the following tasks:

1. Run the following CLI command to get list of aliases having Mailbox Status field set as non-zero: run **cuc dbquery unitydirdb** select y.alias from vw_mailboxmap as x, vw_user as y where x.userobjectid=y.objectid AND x.status != 0.
2. If the above CLI execution gives list of user aliases then we need to check the reason of non-zero value of status for listed users. If required we can update the status field to zero through the following CLI command: run **cuc dbquery unitydirdb** update tbl_mailboxmap set status = 0

Note Updating the value of "status" as zero is just a work around and we must investigate the reason of status getting changed.

Single Inbox Synchronization from Office 365 Is Delayed

If Connection synchronization to Office 365 is working (for example, voice messages are synchronized to users' Exchange mailboxes) but synchronization from Office 365 is delayed (for example, the message waiting indicator is not turned off immediately after the last Connection voice message is heard in ViewMail for Outlook), do the following tasks.

1. In Cisco Unity Connection Administration, display the unified messaging account for one of the affected users, and select **Reset**.

If synchronization from Exchange to Connection starts working for the affected user, in Connection Administration, display the unified messaging service associated with the affected user (Unified Messaging > Unified Messaging Services), and select **Reset**

Troubleshooting Problems with Cisco ViewMail for Microsoft Outlook

See the following sections:

Messages Are Not Received

- Voice Messages or Receipts Are Not Received in the Outlook Inbox in Cisco Unity Connection, page 7-10
- Messages Sent From a Single Inbox Outlook Client Are Not Received in Cisco Unity Connection, page 7-10

Messages Go to the Wrong Place

- Messages Are Received in an Email Account Other Than the Single Inbox Account in Cisco Unity Connection, page 7-11

Messages Cannot Be Played

- Messages Cannot Be Played in Outlook for Cisco Unity Connection, page 7-11
- Messages Moved into a .PST Folder in Outlook Can No Longer Be Played in Cisco Unity Connection, page 7-11

Message Waiting Indicators Are Wrong

- Playing a Message Does Not Turn Off the Message Waiting Indicator in Cisco Unity Connection, page 7-12

- Message Waiting Indicator Turns Off Before the Message Is Played in Cisco Unity Connection, page 7-12

Messages Are Not Deleted, or Messages Are Deleted Unexpectedly

- Deleting a Message in Outlook Does Not Delete the Corresponding Message in Cisco Unity Connection, page 7-12
- Messages Moved into a .PST Folder in Outlook Are Deleted in Cisco Unity Connection, page 7-13

Password Troubles

- Troubleshooting Problems with Invalid Passwords in Connection, page 7-13

Diagnostics

- Collecting Diagnostics from ViewMail for Outlook on the User Workstation, page 7-14
- Collecting Diagnostics on the Cisco Unity Connection Server for Problems with Single Inbox and ViewMail for Outlook, page 7-14

Voice Messages or Receipts Are Not Received in the Outlook Inbox in Cisco Unity Connection

If single inbox users do not receive incoming voice messages or receipts in the Outlook Inbox, note the following:

- Check the Junk E-mail folder to see whether the messages or receipts are automatically being filtered to this folder. The junk-email filter can be updated to add specific sender addresses or domain names to the safe filter list. For information on configuring the Junk E-mail folder to exclude a class of messages, refer to the Microsoft documentation.
- Check the configuration of any email anti-spam filters in your organization to see whether voice messages are being routed to a location other than the Outlook Inbox folder, .wav attachments are being removed, or the policy is otherwise interfering with the delivery of voice messages or receipts to Outlook.
- If you have Connection mailbox quotas configured, and if a user has exceeded the send/receive quota, Connection will prevent messages from being received in the user's Connection mailbox. ViewMail for Outlook does not notify a user that the send/receive threshold has been reached and that callers are therefore not allowed to leave voice messages for that user; the user would know only by checking voice messages in Connection. However, when a user sends a message after reaching the send quota, ViewMail for Outlook does notify the user. The send quota is a lower threshold, so a user reaches the send/receive quota only by ignoring the earlier warning.

Messages Sent From a Single Inbox Outlook Client Are Not Received in Cisco Unity Connection

If single inbox users cannot send messages through the Cisco Unity Connection server from the Outlook client—for example, users receive non-delivery receipts (NDRs)—consider the following possibilities:

- The email address of the message sender must exactly match a primary or proxy SMTP address configured in Connection.
- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found, Connection relays the message to the SMTP smart host, or sends an NDR

to the sender, depending on the option selected in the When a Recipient Cannot be Found setting on the System Settings > General Configuration page in Connection Administration. By default, Connection sends an NDR.

Messages Are Received in an Email Account Other Than the Single Inbox Account in Cisco Unity Connection

If users unexpectedly receive voice messages in their corporate or other email accounts rather than their Cisco Unity Connection mailboxes, consider the following possibilities:

- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found and Connection is configured to relay the message to the SMTP smart host, the message is relayed to the applicable email address. Confirm that the message recipient has a proxy SMTP address configured for the applicable email address. See the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
- If message actions for the recipient are configured to relay messages of a particular type (voice, email, fax or delivery receipt) to the user at the corporate email address, the seemingly erroneous routing of messages may be expected behavior. Message actions are also configured in the unified messaging service that is specified in the recipient's unified messaging account, and the interaction of the user-level setting and the setting in the unified messaging service may produce unanticipated results. For a summary of how message actions are relaying messages for a specific user, in Connection Administration, see the Message Actions page for that user.

Messages Cannot Be Played in Outlook for Cisco Unity Connection

To play secure messages from Outlook, you must install Cisco Unity Connection ViewMail for Microsoft Outlook version . When you view a secure message in Outlook, the text in the message briefly explains secure messages but does not include a .wav attachment. The only copy of the .wav file remains on the Connection server.

Caution If you delete a secure message from Outlook, Connection moves the message to the deleted items folder in Connection. If message aging is configured, the message will eventually be deleted.

Messages Moved into a .PST Folder in Outlook Can No Longer Be Played in Cisco Unity Connection

Connection synchronizes voice messages in the following Outlook folders with the Connection Inbox folder for the user, so the messages are still visible in the Connection Inbox folder:

- Subfolders under the Outlook Inbox folder
- Subfolders under the Outlook Deleted Items folder
- The Outlook Junk Email folder

Beginning with Cisco Unity Connection 9.0 and later, Connection synchronizes voice messages in the Sent Items Outlook folder with the Connection Sent Items folder for the user, so the messages are still visible in the Connection Sent Items folder.

When Connection replicates a secure voice message to Exchange, the replicated message contains only text that briefly explains secure messages; the only copy of the .wav file remains on the Connection server. When a user plays a secure message by using ViewMail for Outlook, ViewMail retrieves the message from the Connection server and plays it without ever storing the message in Exchange or on the computer of the user.

If the user moves a secure message to an Outlook folder that is not synchronized with the Connection Inbox folder, the only copy of the voice message is moved to the deleted items folder in Connection, and the message can no longer be played in Outlook. If the user moves the message back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Connection Inbox folder, and:

- If the message is still in the deleted items folder in Connection, the message is synchronized back into the Connection Inbox for that user, and the message becomes playable again in Outlook.
- If the message is not still in the deleted items folder in Connection, the message is not resynchronized into Connection and can no longer be played in Outlook or Connection.

For more information, see the "How Synchronization Works With Outlook Folders" section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

Playing a Message Does Not Turn Off the Message Waiting Indicator in Cisco Unity Connection

If you upgraded from Cisco Unity, if you migrated messages, and if the Cisco Unity server was configured as unified messaging, note the following:

- Two copies of migrated messages will appear in the Exchange mailbox for each user: the original message and the migrated message that is synchronized into the Exchange mailbox when single inbox is configured.
- If a user uses Outlook to play the original message in Exchange (the copy that Cisco Unity put into Exchange when the message was received), the message will remain unread in Connection, and the message waiting indicator will remain on. Playing the migrated message (the copy that was synchronized into the Exchange mailbox by the single inbox feature) or playing messages that are received after the migration will turn off the message waiting indicator as appropriate.

Message Waiting Indicator Turns Off Before the Message Is Played in Cisco Unity Connection

If you have enabled the Outlook option Mark Items as Read When Viewed in the Reading Pane, the message is marked as read as soon as you select it in the Outlook inbox. If this is the only Connection voice message that you have not heard, Connection turns off the message waiting indicator.

Deleting a Message in Outlook Does Not Delete the Corresponding Message in Cisco Unity Connection

If you upgraded from Cisco Unity, if you migrated messages, and if the Cisco Unity server was configured as unified messaging, note the following:

- Two copies of migrated messages will appear in the Exchange mailbox for each user: the original message and the migrated message that is synchronized into the Exchange mailbox when single inbox is configured.

- If a user uses Outlook to delete the original message in Exchange (the copy that Cisco Unity put into Exchange when the message was received), the migrated message will remain in the user's inbox in Connection. Deleting the migrated message in Outlook (the copy that was synchronized into the Exchange mailbox by the single inbox feature) will cause the message to be moved from the user's inbox in Connection to the user's deleted items folder in Connection.

Messages Moved into a .PST Folder in Outlook Are Deleted in Cisco Unity Connection

Connection synchronizes voice messages in the following Outlook folders with the Connection Inbox folder for the user, so the messages are still visible in the Connection Inbox folder:

- Subfolders under the Outlook Inbox folder
- Subfolders under the Outlook Deleted Items folder
- The Outlook Junk Email folder

If a user moves voice messages into Outlook folders that are not under the Inbox folder, the messages are moved to the deleted items folder in Connection.

For more information, see the "How Synchronization Works With Outlook Folders" section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

Troubleshooting Problems with Invalid Passwords in Connection

When users change their Cisco Personal Communications Assistant (PCA) password in the Messaging Assistant, they also must update the password configured in ViewMail options so that the client can continue to access Connection and retrieve voice messages. Likewise, when LDAP authentication is configured and the PCA password is changed in LDAP, the password configured in ViewMail options must be updated. If the PCA password has been changed but ViewMail has not been updated, users typically see a message indicating that the invalid credentials were entered for the account when they try to use ViewMail features.

Do the following procedure to change the password in the user's Outlook client.

To Change a Cisco ViewMail for Microsoft Outlook Password

Step 1 If you are using Outlook 2010:

a. On the user workstation, in Outlook 2010, click the **ViewMail** tab.

b. Select **Settings**.

If you are using Outlook 2007 or Outlook 2003:

a. On the user workstation, on the Outlook Tools menu, select **Options**.

b. Select the **ViewMail** tab.

Step 2 From the Associated Email Account list, select the Microsoft Exchange/Single Inbox account for the user, and select **Edit**.

Step 3 On the Viewmail Account Settings window, change the password for the user.

Step 4 Select **Test Settings**.

Step 5 If the test passes successfully, select **OK**. If the test fails, reenter the password and repeat

Step 6 Select **OK** to close the window, and then select **OK** again to close the Options dialog.

Collecting Diagnostics from ViewMail for Outlook on the User Workstation

To troubleshoot problems with the Cisco ViewMail for Microsoft Outlook form, you can enable diagnostics on the user workstation.

To Enable Cisco ViewMail for Microsoft Outlook Diagnostics and View the Log Files on the User Workstation

Step 1 If you are using Outlook 2010:

a. On the user workstation, in Outlook 2010, click the **ViewMail** tab.

b. Select **Settings**.

If you are using Outlook 2007 or Outlook 2003:

a. On the user workstation, on the Outlook Tools menu, select **Options**.

b. Select the **ViewMail** tab.

Step 2 Check the **Turn on Diagnostic Traces** check box.

Step 3 Select **OK**.

Step 4 Reproduce the problem.

Step 5 If you are using Outlook 2010:

a. On the user workstation, in Outlook 2010, click the **ViewMail** tab.

b. Select **Email Log Files**, and send the resulting message with logs attached to an email address.

If you are using Outlook 2007 or Outlook 2003:

a. On the **Help** menu, select **Cisco ViewMail for Outlook > Email Log Files**.

b. Send the resulting message with logs attached to an email address.

Collecting Diagnostics on the Cisco Unity Connection Server for Problems with Single Inbox and ViewMail for Outlook

You can enable the Cisco Unity Connection VMO macro trace to troubleshoot client problems from the server side.

For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Single Inbox Is Not Working for Anyone on a Connection Server

When single inbox is not working for any of the users on a Connection server (for example, Connection voice messages are not synchronized into Office 365, and messages sent from ViewMail for Outlook are not delivered), do the following tasks.

1. On the primary server, in Cisco Unity Connection Serviceability, go to **Tools > Service Management**, and confirm that the service status for the following services is Started:

  - Connection Mailbox Sync (in the Critical Services section)

2. If a firewall is configured between the Connection and Exchange servers or between Connection and Active Directory domain controllers, confirm that the necessary ports are opened. For more information, see the "IP Communications Required by Cisco Unity Connection 9.x" chapter in the *Security Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.

Troubleshooting Calendar Integrations in Cisco Unity Connection

See the following sections for information on troubleshooting problems with calendar integrations:

How Unified Messaging Accounts Are Used for Calendar Integrations

The following configuration principles apply to unified messaging accounts that are used for calendar integrations:

- A user can have only one unified messaging account for which the Access Exchange Calendar and Contacts check box is checked on the Unified Messaging Accounts page for the user.
- A user can have multiple unified messaging accounts for which the MeetingPlace Scheduling and Joining check box is checked on the Unified Messaging Services page.
- If a user has more than one unified messaging account for which the MeetingPlace Scheduling and Joining check box is checked, the Primary Meeting Service check box (on the Users > Edit Unified Messaging Account page) can be checked on only one of them.

Each user can access calendar information from only one unified messaging account. If the calendar-enabled unified messaging account connects to an Exchange server, the user has access to events only from the Exchange calendar. Similarly, if the calendar-enabled unified messaging account connects to a Cisco Unified MeetingPlace server, the user has access to events only from the Cisco Unified MeetingPlace calendar.

If a user has more than one unified messaging account for which the MeetingPlace Scheduling and Joining check box is checked, the unified messaging account for which the Primary Meeting Service check box is checked determines which Cisco Unified MeetingPlace server is used to schedule reservationless meetings.

For information on configuring a calendar integration between Cisco Unity Connection and Exchange, see the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

Testing the Calendar Integration

Do the following procedure to test the calendar integration.

To Test the Calendar Integration

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

Step 2 On the Search Users page, select the alias of a user.

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

Step 3 On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4 On the Unified Messaging Accounts page, select the name of the applicable external service account.

Step 5 On the Edit Unified Messaging Account page, select **Test**.

Step 6 In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

Step 7 Repeat Step 5 and Step 6 until the test succeeds.

Obtaining Unified Messaging Account Status

In Cisco Unity Connection Administration, browse to the Unified Messaging > Unified Messaging Accounts Status page. The status icon on the page indicates the state of the Cisco Unity Connection configuration.

The Unified Messaging Accounts page for an individual user also displays Connection configuration status.

Test Fails the Last Check (Exchange 2003 Only)

When you select Test on the Edit Unified Messaging Account page to troubleshoot a calendar integration and all checks succeed except for the last check (which fails with the message "The system failed to perform a typical calendar operation"), use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting When the Test Fails the Last Check

1. On the Exchange server, confirm that SP2 or later is installed.
2. On the Exchange server, confirm that the user is enabled for Outlook Web Access (OWA).

3. In Cisco Unity Connection Administration, on the Users > Edit Unified Messaging Account page for the user, confirm that the entry in the Email Address field matches the primary SMTP address for the user.
4. On the Exchange server, confirm that the Microsoft Exchange Outlook Web Access service is available.

   You can manually check whether the Microsoft Exchange Outlook Web Access service is available by entering one of the following URLs in a web browser:

   http://<servername>/exchange/<emailaddress>

   https://<servername>/exchange/<emailaddress>

   Note the following:

   - If the unified messaging account in which the Access Exchange Calendar and Contacts check box is checked is associated with a unified messaging service in which the value of the Web-Based Protocol list is "HTTPS," the URL must begin with "https".
   - If you chose to specify an Exchange Server on the Unified Messaging > Unified Messaging Services page, for <servername>, enter the value of the Exchange Server. Use the unified messaging service to which the unified messaging account of the user refers. If you chose to search for Exchange servers, verify that you can ping the domain, and that the protocol (LDAP or LDAPS) is correct.
   - For <emailaddress>, enter the email address that the user's unified messaging account is using. See the Account Information section of the Users > Edit Unified Messaging Account page for the user. When prompted to authenticate, enter the user's Active Directory alias and password.
5. In Cisco Unified Operating System Administration, on the Services > Ping Configuration page, confirm that Connection can ping the IP address or hostname of the Exchange server.
6. If the unified messaging service is configured to use HTTPS for the web-based protocol and the Validate Certificates for Exchange Servers check box is checked, determine whether certificate validation is causing the problem by doing the following sub-tasks.

   a. In Connection Administration, browse to the Unified Messaging > Unified Messaging Services page, and select the unified messaging service associated with the unified messaging account that you are testing.
   b. On the Edit Unified Messaging Service page, uncheck the **Validate Server Certificate** check box and select **Save**.
   c. On a phone, sign in as the user who experiences the problem and access calendar information.
   d. If the user is able to access calendar information, confirm that the public root certificate of the Certificate Authority (CA) that issued the Exchange server certificate is installed on Connection as a trusted certificate, that it is self-signed, and that it has not expired.
   e. In Connection Administration, on the System Settings > Unified Messaging Services > Edit Unified Messaging Services page, check the **Validate Server Certificate** check box and select **Save**.
7. Confirm that the service account on Exchange that the unified messaging service uses has the Administer Information Store, Receive As, and Send As permissions allowed.
8. If the Exchange server is slow enough to respond to calendar information requests that Connection times out, in Connection Administration, on the System Settings > Advanced > Unified Messaging Services page, set the TTS and Calendars: Time to Wait for a Response (In Seconds) field to a value greater than 4.

Note Increasing the value of TTS and Calendars: Time to Wait for a Response (In Seconds) may result in delays when accessing calendar information.

Test Succeeds, but the Calendar Integration Still Does Not Work (Exchange 2003 Only)

When you select Test on the Edit Unified Messaging Account page to troubleshoot a calendar integration and all checks succeed but the calendar integration still does not work, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a Calender Integration When the Test Succeeds

1. In Cisco Unity Connection Administration, browse to the Unified Messaging > Unified Messaging Services page, and select the unified messaging service associated with the unified messaging account that you are testing. On the Edit Unified Messaging Service page, confirm that the fully qualified DNS name (FQDN) of the Exchange server is resolvable via DNS.
2. Even if the unified messaging service is configured with the IP address of the Exchange server, calendar information from the Exchange server is provided with URLs that contain the FQDN of the server. Connection uses these URLs, which must be resolved by a DNS server so that the user can access calendar information. If the Exchange server is slow enough to respond to calendar information requests that Connection times out, in Connection Administration, on the System Settings > Advanced > Unified Messaging Services page, set the TTS and Calendars: Time to Wait for a Response (In Seconds) field to a value greater than 4.

   Note Increasing the value of TTS and Calendars: Time to Wait for a Response (In Seconds) may result in delays when accessing calendar information.

3. Confirm that the system clocks on the Connection and Exchange servers are both correct.
4. Confirm that the meetings appear on the Outlook calendar of the user.

   If Cisco Unified MeetingPlace meetings are scheduled through the user web interface for these applications, the scheduled meetings do not appear on the Outlook calendar of the user. If you configure the profile for Cisco Unified MeetingPlace with an email type of “Exchange,” meeting requests appear on the Outlook calendar of the user.

Non-Published Meetings Do Not Appear in List of Meetings (Cisco Unified MeetingPlace Only)

When Cisco Unity Connection has an calendar integration with Cisco Unified MeetingPlace, all applicable published and non-published meetings are listed when the user accesses meeting information.

If non-published meetings are not listed in the list of meetings, the service account that Connection uses to access calendar information is not correctly configured. Do the following procedure to configure the service that Connection uses.

To Configure the Connection Service Account (Cisco Unified MeetingPlace Only)

Step 1 Sign in to the Cisco Unified MeetingPlace Administration Server as an administrator.

Step 2 Select **User Configuration > User Profiles**.

Step 3 Select the Connection service account.

Step 4 In the Type of User field, select **System Administrator**.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace.

Meetings Do Not Appear in List of Meetings

When meetings do not appear in the list of meetings, the cause may be the interval that Cisco Unity Connection waits to update calendar information. Do the following procedure.

To Change the Interval That Cisco Unity Connection Waits to Update Calendar Information

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Unified Messaging Services**.

Step 2 On the Unified Messaging Services Configuration page, in the Calendars: Normal Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner. A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.

Step 3 In the Calendars: Short Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

This setting applies to users who have the Use Short Calendar Caching Poll Interval check box checked on their Edit User Basics page.

Step 4 Select **Save**.

"Access Exchange Calendar and Contacts" Option Is Not Available for Unified Messaging Accounts

When the Access Exchange Calendar and Contacts check box does not appear on the Unified Messaging Account page, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a Unified Messaging Service That Cannot Be Saved

1. In Cisco Unity Connection Administration, browse to the Unified Messaging > Unified Messaging Services page, and select the unified messaging service associated with the unified messaging account that you are testing.
2. On the Edit Unified Messaging Service page, confirm that the Access Exchange Calendar and Contacts check box is checked.

Using Traces to Troubleshoot a Calendar Integration

You can use traces to troubleshoot a calendar integration. For detailed instructions, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

Troubleshooting Access to Calendar Information When Using Personal Call Transfer Rules in Cisco Unity Connection

When users have problems accessing calendar information when using Personal Call Transfer Rules, the cause may be the interval that Cisco Unity Connection waits to update calendar information. Do the following procedure.

To Change the Interval That Cisco Unity Connection Waits to Update Calendar Information

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Unified Messaging Services**.

Step 2 On the Unified Messaging Services Configuration page, in the Calendars: Normal Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner. A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.

Step 3 In the Calendars: Short Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

This setting applies to users who have the Use Short Calendar Caching Poll Interval check box checked on their Edit User Basics page.

Step 4 Select **Save**.

You can use traces to troubleshoot issues related to accessing calendar information when using personal call transfer rules. For detailed instructions, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

See also the "Troubleshooting Personal Call Transfer Rules in Cisco Unity Connection 9.x" chapter.

CHAPTER 8

Troubleshooting Microsoft Office 365 for Unified Messaging in Cisco Unity Connection

Revised December 12, 2012

See the following sections:

Single Inbox Is Not Working for Anyone on a Connection Server

When single inbox is not working for any of the users on a Connection server (for example, Connection voice messages are not synchronized into Office 365, and messages sent from ViewMail for Outlook are not delivered), do the following tasks.

1. On the primary server, in Cisco Unity Connection Serviceability, go to **Tools > Service Management**, and confirm that the service status for the following services is Started:
   - Connection Mailbox Sync (in the Critical Services section)
2. If a firewall is configured between the Connection and Exchange servers or between Connection and Active Directory domain controllers, confirm that the necessary ports are opened. For more information, see the "IP Communications Required by Cisco Unity Connection 9.x" chapter in the *Security Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.

Single Inbox Is Not Working for Users Associated with a Unified Messaging Service

When single inbox is not working (for example, Connection voice messages are not synchronized into Office 365, and messages sent from ViewMail for Outlook are not delivered), and when the problem is occurring only for the Connection users whose unified messaging accounts are associated with the same unified messaging service, do the following tasks.

Note When a cluster is configured, do the Connection-specific tasks only on the primary (active) server.

1. Confirm that the unified messaging service is enabled and that single inbox is enabled:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, confirm that the **Enabled** check box is checked.
   b. Confirm that the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box is checked.
2. Test the unified messaging service:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, select **Test**.
   b. Correct any problems that are listed on the Task Execution Results page.
3. Test one of the affected unified messaging accounts:
   a. In Connection Administration, on the **Users > Edit User Basics > Unified Messaging Accounts** page, select **Test**.
   b. Correct any problems that are listed on the Task Execution Results page. Among the problems that the Task Execution Results page may list are the following browser errors:

      401 error: Possible causes include an incorrect password for the unified messaging services account, an incorrect username, or an invalid format for the username.

      403 error: SSL is required in Office 365, but the public certificates from the certification authority (CA) that signed the certificates on the Office 365 servers have not been uploaded to the Connection server.

      456 error: Possible causes include expiration of service account. Reset the password on the Office 365 server.
4. In Cisco Unity Connection Serviceability, go to **Tools > Service Management**. In the Critical Services section, confirm that the service status for the Connection Mailbox Sync service is Started.
5. Check the Active Directory settings on the unified messaging services account:
   – Confirm that the account is not locked.
   – Confirm that the password for the account has not expired.
6. Temporarily replace the unified messaging services account with the Active Directory account for a Connection:
   a. In Connection Administration, on the **Unified Messaging > Unified Messaging Services > Edit Unified Messaging Service** page, in the Username and Password fields, replace the credentials for the unified messaging services account with the credentials for a Connection user associated with this unified messaging service.
   b. Send the user a Connection voice message, and determine whether the voice message synchronized to Office 365.

      If the message did not synchronize, switch the Username and Password fields back to the values for the unified messaging services account, then skip to Task 7

      If the message did synchronize, the problem is probably with permissions on the unified messaging services account. Continue with Task 6.c.
   c. Switch the Username and Password fields back to the values for the unified messaging services account.

d. Send the Connection user another voice message, and determine whether the voice message synchronized to Office 365.

   If the message did synchronize, test with some other users who are associated with the same unified messaging service to ensure that the problem is resolved.

7. Use Microsoft EWSEditor to try to access the Exchange mailbox of a Connection user by using the unified messaging services account. This allows you to determine whether the problem occurs even when Connection is not involved.

   EWSEditor software and documentation are available on the Microsoft website www.testexchangeconnectivity.com.

Single Inbox Synchronization from Office 365 Is Delayed

If Connection synchronization to Office 365 is working (for example, voice messages are synchronized to users' Office 365 mailboxes) but synchronization from Office 365 is delayed (for example, the message waiting indicator is not turned off immediately after the last Connection voice message is heard in ViewMail for Outlook), do the following tasks.

1. In Cisco Unity Connection Administration, display the unified messaging account for one of the affected users, and select **Reset**.

   If synchronization from Exchange to Connection starts working for the affected user, in \, display the unified messaging service associated with the affected user (Unified Messaging > Unified Messaging Services), and select **Reset**.

You may experience delay (in order of hours) in synchronization of voice messages from Office 365 server to Connection while **Resynchronize All Single-Inbox Messages SysAgent** task is running. It is recommended to run **Resynchronize All Single-Inbox Messages SysAgent task** during off hours.

Consider Table 8-1 as an example for 3000 and 5000 Office 365 users.

Table 8-1 Example

Office365 Users	VoiceMail Count (Size)	Latency (Millisecond)	RESYNC TIME (MINUTES)
3000	2,39,657 (231 KB)	300	130
5000	2,39,657 (231 KB)	300	210

Note The resynchronization time of voice messages from Office 365 server to Connection depends upon the following factors:

- Number of CAS servers/Arrays
- Number of messages that are out of sync(states) per mailbox
- CAS performance
- Latency between Connection and 0ffice 365

Single Inbox Fails with Office 365 When ADFS Is Used

Added December 12, 2012

The Single Inbox may not work, if you are integrating Cisco Unity Connection with Office 365 for Single Inbox where the Unity Connection Account used to access Office 365 was created on active directory and imported into Office 365, as Connection is not equipped to handle ADFS.

To get the Single Inbox working, the account must be created locally on the Office 365 side.

Resolving SMTP Domain Name Configuration Issues

To resolve SMTP Domain Name configuration issues

Step 1 In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Smart Host**.

Step 2 On the Smart Host page, in the Smart Host field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

Step 3 Click on Save.

Step 4 In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

Step 5 On the General Configuration page, in the **When a recipient cannot be found** list, select **Relay message to smart host**.

Step 6 Click on Save.

Step 7 In Cisco Unity Connection Administration, expand **Users > Message Actions**. Select the Accept the message option from the Voicemail drop- down list.

Note Do not create any SMTP Proxy Address for the user .Make sure to select the Relay the message option from the Email, Fax, and receipt drop -down lists.

Step 8 On Exchange 2010 server, make sure to configure the SMTP Proxy addresses for Connection Publisher and Subscriber servers.

Step 9 On Exchange 2010 server, setup a recipient policy such that the Cisco Unity Connection alias resolves to the corporate email Id. For details, see the following link:

http://technet.microsoft.com/en-us/library/bb232171.aspx

Note We recommend that you do not configure the above steps while using secure voice messages because they will be replicated to Exchange.

CHAPTER 9

Troubleshooting the Phone System Integration in Cisco Unity Connection 9.x

See the following sections:

Diagnostic Tools in Cisco Unity Connection 9.x

There are diagnostic tools available to help you troubleshoot phone system integrations:

Configuring Cisco Unity Connection for the Remote Port Status Monitor

You can use the Remote Port Status Monitor for a real-time view of the activity of each voice messaging port on Cisco Unity Connection. This information assists you in troubleshooting conversation flow and other problems.

After installing the Remote Port Status Monitor on your workstation, do the following procedure to configure Connection.

Note For detailed information on using the Remote Port Status Monitor, see the training and Help information available at http://www.ciscounitytools.com/Applications/CxN/PortStatusMonitorCUC7x/PortStatusMonitorCUC7x.html.

To Configure Cisco Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Conversations**.

Step 2 On the Conversation Configuration page, check the **Enable Remote Port Status Monitor Output** check box.

Step 3 In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations.

Note that you can enter up to 70 IP addresses. Each IP address must be separated from the following IP address by a comma.

Step 4 Select **Save**.

Using the Check Telephony Configuration Test

You can use the Check Telephony Configuration test to troubleshoot the phone system integration.

For example, use this test if the following conditions exist:

- Calls to Cisco Unity Connection are failing.
- Ports are failing to register.

Do the following procedure.

To Use the Check Telephony Configuration Test

Step 1 In Cisco Unity Connection Administration, in the Related Links box in the upper right corner of any Telephony Integrations page, select **Check Telephony Configuration** and select **Go**.

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

Step 2 In the Task Execution Results window, select **Close**.

Troubleshooting Call Control in Cisco Unity Connection 9.x

Use the following troubleshooting information if the phone system integration has problems related to call control. Do the following tasks, as applicable:

- Use the Check Telephony Configuration test. See the "Using the Check Telephony Configuration Test" section on page 9-2.
- Use traces to troubleshoot call control issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Traces in Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x" section on page 2-1.

- *(Cisco Unified Communications Manager integrations only)* If you hear a fast busy tone when you call Cisco Unity Connection, verify the configuration for the phone system integration. See the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Cisco Unity Connection 9.x Is Not Answering Any Calls

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

To Verify the Phone System Settings in Cisco Unity Connection Administration

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

Step 2 On the applicable pages, confirm that the settings for the phone system, port groups, and ports match those indicated in the integration guide for your phone system.

Step 3 Correct any incorrect values in Connection Administration. If you change any values, select **Save** before leaving the page.

Step 4 If prompted to reset a port group, on the applicable Port Group Basics page, select **Reset**. Otherwise, continue to Step 5.

Step 5 In the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the phone system integration settings.

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

Step 6 In the Task Execution Results window, select **Close**.

Cisco Unity Connection 9.x Is Not Answering Some Calls

When Cisco Unity Connection is not answering some calls, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Sporadic Answers on Incoming Calls

1. Confirm that the routing rules are working correctly. See the "Confirming Routing Rules" section on page 9-3.
2. Confirm that calls are sent to the correct voice messaging ports and that the ports are enabled. See the "Confirming Voice Messaging Port Settings" section on page 9-4.

Confirming Routing Rules

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

Use traces to troubleshoot issues with routing rules. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Traces in Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x" section on page 2-1.

Confirming Voice Messaging Port Settings

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

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

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

Step 2 On the Search Ports page, note which ports are designated to answer calls.

Step 3 On the phone system, in the phone system programming, confirm that calls are being sent only to those voice messaging ports that are designated to answer calls. Change the phone system programming if necessary.

If a voice messaging port is disabled or set incorrectly, it does not answer calls. Do the following procedure.

To Confirm That Voice Messaging Ports Are Enabled

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

Step 2 On the Search Ports page, review the Enabled column.

Step 3 If a voice messaging port is not enabled and should be in use, select the display name of port.

Step 4 On the Port Basics page for the port, check the **Enabled** check box to enable the port.

Step 5 On the Port menu, select **Search Ports**.

Step 6 Repeat Step 3 through Step 5 for all remaining ports that should be in use.

Troubleshooting an Integration of Cisco Unity Connection 9.x with Cisco Unified Communications Manager

See the following sections for information on troubleshooting a Cisco Unified Communications Manager integration:

Viewing or Editing the IP Address of a Cisco Unified Communications Manager Server

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

To Change Cisco Unified Communications Manager Server Settings

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

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

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

Step 4 On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and select **Save**.

Step 5 If no status message appears, skip the remaining steps in this procedure. If a status message appears prompting you to reset the port group, on the Edit menu, select **Port Group Basics**.

Step 6 On the Port Group Basics page, under Port Group, select **Reset**.

Ports Do Not Register or Are Repeatedly Disconnected in an SCCP Integration

When the Cisco Unity Connection voice messaging ports do not register with Cisco Unified CM in an SCCP integration, or if the Connection ports repeatedly disconnect from Cisco Unified CM in an SCCP integration, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Port Registration Problems

1. Test the port group. See the "Testing the Port Group" section on page 9-5.
2. Confirm that another port group on the Connection server does not use the same device name prefix to connect ports to the Cisco Unified CM server. See the "Confirming That Another Port Group Does Not Use the Same Device Name Prefix" section on page 9-6.
3. Confirm that another Connection server does not use the same device name prefix to connect its ports to the Cisco Unified CM server. See the "Confirming That Another Cisco Unity Connection Server Does Not Use the Same Device Name Prefix" section on page 9-7.

Testing the Port Group

Do the following procedure.

To Test the Port Group

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

Step 2 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 3 On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.

Note On the Port Basics page, you can test a single port in an SCCP integration by selecting **Test Port** in the Related Links list and selecting **Go**.

Note The Test Port and Test Port Group utilities do not test IPv6 connectivity. Even when Connection is configured to use IPv6 for a SCCP integration, the tests confirm that Connection can communicate with the phone system by using IPv4 addressing.

Step 4 When prompted that the test will terminate all calls in progress, select **OK**.

The Task Execution Results displays one or more messages with troubleshooting steps.

Step 5 Follow the steps for correcting the problems.

Caution If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test will fail. You must configure Cisco Unified CM and the system to enable pings so that the test can accurately test the port registration.

Step 6 Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

Confirming That Another Port Group Does Not Use the Same Device Name Prefix

Do the following procedure.

To Confirm That Another Port Group Does Not Use the Same Device Name Prefix

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

Step 2 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 3 On the Port Group Basics page, note the value of the Device Name Prefix field.

Caution This value of the Device Name Prefix field must be unique for each port group. Otherwise, more than one port may attempt to connect to an SCCP device, causing the ports to repeatedly disconnect from Cisco Unified CM and to disconnect calls that the ports are handling.

Step 4 Select **Next** to view the next port group for which the integration method is SCCP (Skinny).

Step 5 If the value of the Device Name Prefix field is different from the value that you noted in Step 3, skip to Step 8. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.

Step 6 Select **Save**.

Step 7 Select **Reset**.

Step 8 Repeat Step 4 through Step 7 for all remaining port groups for which the integration method is SCCP (Skinny).

Confirming That Another Cisco Unity Connection Server Does Not Use the Same Device Name Prefix

Do the following procedure.

To Confirm That Another Cisco Unity Connection Server Does Not Use the Same Device Name Prefix

Step 1 In Cisco Unity Connection Administration on the first Cisco Unity Connection server, expand **Telephony Integrations**, then select **Port Group**.

Step 2 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 3 On the Port Group Basics page, note the value of the Device Name Prefix field.

Step 4 In Cisco Unity Connection Administration on the second Connection server, expand **Telephony Integrations**, then select **Port Group**.

Step 5 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 6 On the Port Group Basics page, note the value of the Device Name Prefix field.

Caution The value of the Device Name Prefix field must be unique for each port group. Otherwise, more than one port may attempt to connect to an SCCP device, causing the ports to repeatedly disconnect from Cisco Unified CM and to disconnect calls that the ports are handling.

Step 7 If the value of the Device Name Prefix field you noted in Step 6 is different from the value you noted on the first Connection server in Step 3, skip to Step 10. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.

Step 8 Select **Save**.

Step 9 Select **Reset**.

Step 10 Select **Next**.

Step 11 Repeat Step 7 through Step 10 for all remaining port groups for which the integration method is SCCP (Skinny).

Ports Do Not Register in an IPv6 Configuration

When the Cisco Unity Connection voice messaging ports do not register with Cisco Unified CM in an integration that is configured to use IPv6 addressing, and the CsMgr logs errors in the application syslog during startup, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Port Registration Problems in an IPv6 Configuration

1. Confirm that IPv6 is enabled.
   - To check by using the command-line interface (CLI), enter **show network ipv6 settings**.
   - To check by using Cisco Unified Operating System Administration, see the "Confirming that IPv6 is Enabled by Using Cisco Unified Operating System Administration" section on page 9-8.
2. Confirm that Connection is configured to use the appropriate addressing mode and preferences. See the "Confirming the IPv6 Addressing Mode and Preferences Settings" section on page 9-8
3. If you have configured an IPv6 host name for the Connection and/or Cisco Unified CM servers rather than configuring by IPv6 address, confirm that the DNS server can resolve the host name properly. To check by using the CLI, enter **utils network ipv6 ping** <IPv6 host name>.
4. If you have configured the port group(s) in Connection with an IPv6 host name for the Cisco Unified CM server(s) rather than with an IPv6 address, confirm that the DNS server can resolve the Cisco Unified CM host name correctly. Likewise, if you have configured Cisco Unified CM to contact the Connection server by IPv6 host name (for example, on a SIP trunk, for the Destination Address IPv6 field), confirm that the DNS server can resolve the Connection host name correctly.
5. Confirm that the Cisco Unified CM server is configured correctly for IPv6, and has the correct settings for signalling and media preferences. See the "Internet Protocol Version 6 (IPv6)" chapter of the applicable *Cisco Unified Communications Manager Features and Services Guide* for your release of Cisco Unified CM, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Confirming that IPv6 is Enabled by Using Cisco Unified Operating System Administration

To Confirm that IPv6 Is Enabled by Using Cisco Unified Operating System Administration

Step 1 In Cisco Unified Operating System Administration, from the Settings menu, select **IP**, then select **Ethernet IPv6**.

Step 2 On the Ethernet IPv6 Configuration page, review the **Enable IPv6** check box, and check it if it is not already checked.

Step 3 If you checked the Enable IPv6 check box in Step 2, configure the Address Source for the Connection server. To apply the change, check Update with Reboot, and select **Save**. The Connection server will reboot in order for the change to take effect.

Confirming the IPv6 Addressing Mode and Preferences Settings

To Confirm the IPv6 Addressing Mode and Preferences Settings

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

Step 2 On the Edit General Configuration page, review the option selected for **IP Addressing Mode**, which controls where Connection listens for incoming traffic:

- IPv4
- IPv6

- IPv4 and IPv6

Step 3 If you change any values on the page, select **Save** to save the changes. When you change the IP Addressing Mode, you must stop and restart the Conversation Manager service on the Tools > Service Management page in Cisco Unity Connection Serviceability in order for the change to take effect.

Step 4 If the IP addressing mode was configured for IPv4 and IPv6 in Step 2, do the following substeps to review the call control signalling and/or media addressing mode settings for the Cisco Unified Communications Manager integration:

a. Expand Telephony Integrations, then select Port Group.

b. On the Search Port Groups page, select the display name of the port group that you want to verify.

c. On the Port Group Basics page, on the Edit menu, select **Servers**.

d. In the IPv6 Addressing Mode section, verify the option selected for the applicable setting(s):

- **Preference for Signaling**—*(Applicable to both SCCP integrations and SIP integrations)* This setting determines the call control signaling preference when registering with Cisco Unified CM via SCCP or when initiating SIP requests.
- **Preference for Media**—*(Applicable only to SIP integrations)* This setting determines the preferred addressing mode for media events when communicating with dual-stack (IPv4 and IPv6) devices.

e. If you made any changes to the page, select **Save**.

Determining the Correct Port Group Template

When adding a phone system integration for Cisco Unified CM, there are two valid options for the Port Group Template field: SCCP or SIP. The SIP port group template is valid only for integrations with Cisco Unified CM 5.0(1) and later.

To integrate Cisco Unity Connection with a phone system through PIMG or TIMG units, in the Port Group Template field, you must select SIP to DMG/PIMG/TIMG.

Problems That Occur When Cisco Unity Connection Is Configured for Cisco Unified Communications Manager Authentication or Encryption

If problems occur when Cisco Unity Connection is configured for Cisco Unified Communications Manager authentication and encryption for the voice messaging ports, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

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

Task List for Troubleshooting Problems When Cisco Unified Communications Manager Authentication or Encryption Is Configured

1. Confirm that the Cisco Unified CM CTL client is configured for mixed mode. See the "Confirming That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode" section on page 9-10.
2. Test the port group configuration. See the "Testing the Port Group Configuration" section on page 9-10.
3. For SCCP integrations, confirm that the security mode setting for the ports in Connection matches the security mode setting for the ports in Cisco Unified CM. See the "Matching the Security Mode Setting for Ports in Cisco Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)" section on page 9-11.
4. For a SIP trunk integration, confirm that the security mode setting for the Connection port group matches the security mode setting for the Cisco Unified CM SIP trunk security profile. See the "Matching the Security Mode Setting for the Cisco Unity Connection Port Group and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-12.
5. For SIP trunk integrations, confirm that the Subject Name field of the Connection SIP certificate matches the X.509 Subject Name field of the Cisco Unified CM SIP trunk security profile. See the "Matching the Subject Name Fields of the Cisco Unity Connection SIP Certificate and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-12.
6. For SIP trunk integrations, confirm that Connection and the SIP trunk use the same port. See the "Matching the Port Used by the Cisco Unity Connection SIP Security Profile and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-13.
7. Copy the Connection root certificate to the Cisco Unified CM servers. See the "Copying the Cisco Unity Connection Root Certificate to the Cisco Unified Communications Manager Servers" section on page 9-13.

Confirming That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode

Do the following procedure.

To Confirm That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **Enterprise Parameters**.

Step 2 On the Enterprise Parameters Configuration page, under Security Parameters, locate the **Cluster Security Mode** field.

Step 3 Confirm that the setting is **1**, which means that the CTL client is configured for mixed mode.

Testing the Port Group Configuration

Do the following procedure.

To Test the Port Group Configuration

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

Step 2 On the Search Port Groups page, select the name of a port group.

Step 3 On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.

Note The Test Port and Test Port Group utilities do not test IPv6 connectivity. Even when Connection is configured to use IPv6 for a SCCP integration, the tests confirm that Connection can communicate with the phone system by using IPv4 addressing.

Step 4 When prompted that the test will terminate all calls in progress, select **OK**.

The Task Execution Results displays one or more messages with troubleshooting steps.

Step 5 Follow the steps for correcting the problems.

Caution If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test will fail. You must configure Cisco Unified CM and the system to enable pings so that the test can accurately test the port registration.

Step 6 Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

Matching the Security Mode Setting for Ports in Cisco Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)

Do the following procedure.

To Match the Security Mode Setting for Ports in Cisco Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select **Cisco Voice Mail Port**.

Step 2 On the Find and List Voice Mail Ports page, select **Find**.

Step 3 In the Device Security Mode column, note the security mode setting for the ports.

Step 4 Sign in to Cisco Unity Connection Administration.

Step 5 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 6 On the Search Ports page, select the name of the first port.

Step 7 On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 3 and select **Save**.

Step 8 Select **Next**.

Step 9 Repeat Step 7 and Step 8 for all remaining ports.

Matching the Security Mode Setting for the Cisco Unity Connection Port Group and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Do the following procedure.

To Match the Security Mode Setting for the Cisco Unity Connection Port Group and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile > SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the Device Security Mode field.

Step 5 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

Step 7 On the Search Port Groups, select the name of the applicable port group.

Step 8 On the Port Group Basics page, in the Security Mode field, select the setting that you noted in Step 4 and select **Save**.

Matching the Subject Name Fields of the Cisco Unity Connection SIP Certificate and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Do the following procedure.

To Match the Subject Name Fields of the Cisco Unity Connection SIP Certificate and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile > SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the X.509 Subject Name field.

Step 5 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificate**.

Step 7 On the Search SIP Certificates page, select the name of the SIP certificate.

Step 8 On the Edit SIP Certificate page, in the Subject Name field, enter the setting that you noted in Step 4 and select **Save**.

Matching the Port Used by the Cisco Unity Connection SIP Security Profile and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Do the following procedure.

To Match the Port Used by the Cisco Unity Connection SIP Security Profile and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile > SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the Incoming Port field.

Step 5 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

Step 7 On the Search SIP Security Profiles page, select the name of the SIP security profile with "TLS."

Step 8 On the Edit SIP Security Profile page, in the Port field, enter the setting that you noted in Step 4 and select **Save**.

Copying the Cisco Unity Connection Root Certificate to the Cisco Unified Communications Manager Servers

Do the applicable procedure:

- To Copy the Root Certificate for Cisco Unified Communications Manager 4.x, page 9-13
- To Copy the Root Certificate for Cisco Unified Communications Manager 5.x, page 9-14
- To Copy the Root Certificate for Cisco Unified Communications Manager 6.x, 7.x, and Later, page 9-15

To Copy the Root Certificate for Cisco Unified Communications Manager 4.x

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Cisco Unity Connection server where you want to save the Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.0** (rather than .htm), and select **Save**.

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

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Cisco Unity Connection root certificate file to the C:\Program Files\Cisco\Certificates folder on all Cisco Unified CM servers in this Cisco Unified CM phone system integration.

Step 7 In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the connection to the Cisco Unified CM servers.

To Copy the Root Certificate for Cisco Unified Communications Manager 5.x

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Cisco Unity Connection server where you want to save the Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.

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

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

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

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

a. On the Cisco Unified CM server, in Cisco Unified Operating System Administration, on the Security menu, select **Certificate Management > Upload Certificate/CTL**.

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

c. Browse to the Cisco Unity Connection root certificate that you saved in Step 4.

d. Follow the on-screen instructions.

e. Repeat Step 6a. through Step 6d. on all remaining Cisco Unified CM servers in the cluster.

f. In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the connection to the Cisco Unified CM servers.

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

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

Step 7 If prompted, restart the Cisco Unity Connection software.

To Copy the Root Certificate for Cisco Unified Communications Manager 6.x, 7.x, and Later

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Cisco Unity Connection server where you want to save the Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.

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

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

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

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

a. On the Cisco Unified CM server, sign in to Cisco Unified Operating System Administration.
b. In Cisco Unified Operating System Administration, on the Security menu, select **Certificate Management**.
c. On the Certificate List page, select **Upload Certificate**.
d. On the Upload Certificate page, in the Certificate Name field, select **CallManager-Trust**.
e. In the Root Certificate field, enter **Cisco Unity Connection Root Certificate**.
f. To the right of the Upload File field, select **Browse**.
g. In the Choose File dialog box, browse to the Cisco Unity Connection root certificate that you saved in Step 4.
h. Select **Open**.
i. On the Upload Certificate page, select **Upload File**.
j. Select **Close**.
k. Restart the Cisco Unified CM server.

l. Repeat Step 6a. through Step 6k. on all remaining Cisco Unified CM servers in the cluster.

m. In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the connection to the Cisco Unified CM servers.

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

n. In the Task Results window, select **Close**.

CHAPTER 10

Troubleshooting Message Waiting Indicators (MWIs) in Cisco Unity Connection 9.x

This chapter describes message waiting indicators (MWIs), what causes Cisco Unity Connection to turn MWIs on and off, and methods for troubleshooting problems with MWIs.

See the following sections:

Triggers for Turning MWIs On and Off in Cisco Unity Connection 9.x

An MWI is a lamp, flashing LCD panel, or special dial tone on user phones that lets users know a voice message is waiting. The type of indicator depends on the phone system and the user phones. Phone systems that support message counts may also display the number of messages that the user has.

MWIs are not the same as message notification, which is the feature that notifies a user of new voice messages by calling a phone, pager, or other device, or by sending an email message.

The following events trigger Cisco Unity Connection to turn MWIs on and off:

- When a message for a user arrives on the Connection message store, Connection notifies the phone system to turn on an MWI on the phone for that user.

  Any message that arrives on the Connection message store (for example, voice messages, emails, and faxes) trigger turning MWIs on and off.
- When the user listens to the message, Connection notifies the phone system to turn off the MWI on the phone.
- When the user saves or deletes a read message, Connection notifies the phone system to turn off the MWI on the phone.
- When a user deletes a new message without listening to it, Connection notifies the phone system to turn off the MWI on the phone.
- When MWIs are synchronized, Connection queries the message store to determine the status of MWIs on all phones, and resets the applicable MWIs.

However, an MWI remains on under the following conditions:

- More messages are waiting to be heard. When all new messages are listened to, the MWI is turned off.
- A new message arrives while the user is listening to the original message. When all new messages are listened to, the MWI is turned off.
- The user listens on the phone to only part of the message, then either hangs up or skips to the next message before hearing the entire message.
- In an email application, in the Cisco Unity Connection Web Inbox, or in the Messaging Inbox , the user marks a listened-to message as unread.

Messages in an external message store do not trigger Connection to turn MWIs on and off.

MWI Problems in Cisco Unity Connection 9.x

See the following sections for information on troubleshooting problems with MWIs:

- MWIs Do Not Turn On or Off, page 10-2
- MWIs Turn On But Do Not Turn Off, page 10-4
- There Is a Delay for MWIs to Turn On or Off, page 10-6
- When the MWI Is On, No Message Count Is Given on the Phone, page 10-7

MWIs Do Not Turn On or Off

When MWIs do not turn on or off, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting When MWIs Do Not Turn On or Off

1. Run the Check Telephony Configuration test. See the "Running the Check Telephony Configuration Test" section on page 10-3.
2. Confirm that there are voice messaging ports for the phone system integration that are assigned to send MWI requests. To view the settings, in Cisco Unity Connection Administration, select **Telephony Integrations > Ports**.

   Note that PIMG/TIMG serial integrations do not send MWI requests through voice messaging ports.
3. Confirm that the voice messaging ports that are assigned to send MWI requests are enabled. To view the settings, in Connection Administration, select **Telephony Integrations > Ports**.

   Note that PIMG/TIMG serial integrations do not send MWI requests through voice messaging ports.
4. Confirm that an adequate number of voice messaging ports for the phone system integration are assigned to send MWI requests. Otherwise, the ports may be too busy to dial out immediately to turn MWIs on and off. To view the ports, in Connection Administration, select **Telephony Integrations > Ports**.

   Note that PIMG/TIMG serial integrations do not send MWI requests through voice messaging ports.
5. Confirm that the port groups for the phone system integration enable MWIs. To view the Enable Message Waiting Indicators check box, in Connection Administration, select **Telephony Integrations > Port Group > Port Group Basics**.

6. *(Cisco Unified CM SCCP integrations only)* Confirm that the settings are correct for the MWI On Extension field and the MWI Off Extension field. To view the Cisco Unified CM settings, in Cisco Unified Communications Manager Administration, select **Voice Mail > Message Waiting**. To view the Connection settings, in Connection Administration, select **Telephony Integrations > Port Group > Port Group Basics**.
7. *(PIMG/TIMG serial integrations only)* Confirm that a separate port group exists to send MWI requests to the master PIMG/TIMG unit. To view the port groups, in Connection Administration, select **Telephony Integrations > Port Group**. For details on the MWI port group, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
8. Confirm that MWIs for the phone system are not forced off. To view the Force All MWIs Off for This Phone System check box, in Connection Administration, select **Telephony Integrations > Phone System > Phone System Basics**.
9. Confirm that the MWI is enabled for the user. To view the Enabled check box, in Connection Administration, select **Users > Users > Messaging Waiting Indicators**.
10. Confirm that the correct phone system is assigned to the MWI for the user. To view the Phone System field, in Connection Administration, select **Users > Users > Messaging Waiting Indicators**.
11. *(Cisco Unified CM SCCP integrations only)* Confirm that the extensions that turn MWIs on and off are in the same calling search space that contains the phones and voicemail ports. From a phone, dial the extension that turns on the MWI. If you hear the reorder tone, the extension for turning on MWIs is not assigned to the correct calling search space in Cisco Unified CM Administration. If you do not hear the reorder tone, but the MWI is not turned on or off, a route plan may be causing the problem.

    To view the calling search space for the MWI extensions, in Cisco Unified CM Administration, select **Voice Mail > Message Waiting**.
12. *(Cisco Unified CM SCCP integrations only)* Confirm that the dial plan does not overlap with the MWI extensions. MWI extensions must be unique. To view the dial plan, in Cisco Unified CM Administration, select **Call Routing > Dial Plan Installer**.
13. *(PIMG/TIMG serial integrations only)* Confirm that the RS-232 serial cable is firmly seated in the serial port of the master PIMG/TIMG unit and in the serial port of the phone system.
14. Verify whether the Connection server was upgraded, restored by using the Disaster Recovery System, or experienced an event that disrupted MWI synchronization. See the "Synchronizing MWIs" section on page 10-4.
15. If the preceding tasks did not resolve the MWI problem, enable macro traces for MWIs. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Running the Check Telephony Configuration Test

Note The Check Telephony Configuration test does not test IPv6 connectivity. (IPv6 is supported in Connection for Cisco Unified Communications Manager integrations.) The test confirms that Connection can communicate with the phone system by using IPv4 addressing.

Do the following procedure.

To Run the Check Telephony Configuration Test

Step 1 In Cisco Unity Connection Administration, in the Related Links list in the upper right corner of any Telephony Integrations page, select **Check Telephony Configuration** and select **Go**.

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

Step 2 In the Task Execution Results window, select **Close**.

Synchronizing MWIs

We recommend resynchronizing MWIs for the system in the following circumstances:

- After a server is restored by using the Disaster Recovery System.
- After upgrading a system.
- After a WAN outage in a system that has distributed voice messaging through Cisco Unified Survivable Remote Site Telephony (SRST) routers or Cisco Unified Communications Manager Express routers in SRST mode.

Do the following procedure.

To Synchronize MWIs for a Phone System Integration

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

Step 2 On the Search Phone Systems page, select the name of the phone system for which you want to synchronize all MWIs.

Step 3 On the Phone System Basics page, under Message Waiting Indicators, select **Run**.

Note that synchronizing MWIs for the phone system may affect system performance. We recommend that you do this task when phone traffic is light.

MWIs Turn On But Do Not Turn Off

Use the troubleshooting information in this section if MWIs turn on but do not turn off. See the following possible causes:

- For PIMG/TIMG integrations, certain phone systems require that Cisco Unity Connection use port memory to turn off MWIs so that the same port is used for turning off an MWI that was used for turning on the MWI. See the "Confirming That Cisco Unity Connection Uses Port Memory (PIMG/TIMG Integrations)" section on page 10-5.
- For PIMG/TIMG integrations, if the phone system requires port memory, one or more of the ports used to set MWIs were deleted or were reconfigured not to set MWIs. You must have the phone system turn off all MWIs, then have Connection resynchronize all MWIs.

  To avoid this problem when deleting or reconfiguring MWI ports not to set MWIs, see the "Deleting or Reconfiguring MWI Ports When Port Memory Is Used (PIMG/TIMG Integrations)" section on page 10-5.

Confirming That Cisco Unity Connection Uses Port Memory (PIMG/TIMG Integrations)

When MWIs turn on but do not turn off, the cause may be port memory. For Avaya, Rolm, and Siemens Hicom phone system integrations, Cisco Unity Connection must use the same port for turning off an MWI that was used for turning on the MWI. When Connection is integrated with one of these phone systems and uses a different port for turning off an MWI, the MWI request for turning off the MWI fails.

Note that this problem does not apply to PIMG/TIMG serial integrations.

If your phone system requires port memory, do the following procedure to confirm that Connection uses port memory.

To Confirm That Cisco Unity Connection Uses Port Memory (PIMG/TIMG Integrations)

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

Step 2 On the Search Phone Systems page, select the name of the phone system.

Step 3 On the Phone System Basics page, under Message Waiting Indicators, confirm that the **Use Same Port for Enabling and Disabling MWIs** check box is checked.

Step 4 Select **Save**.

Deleting or Reconfiguring MWI Ports When Port Memory Is Used (PIMG/TIMG Integrations)

If Cisco Unity Connection must use the same port for turning off an MWI that was used for turning on the MWI, and you want to delete an MWI port or reconfigure an MWI port not to set MWIs, do the applicable procedure.

To Delete MWI Ports When Port Memory Is Used (PIMG/TIMG Integrations)

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

Step 2 On the Search Phone Systems page, select the name of the phone system.

Step 3 On the Phone System Basics page, under Message Waiting Indicators, check the **Force All MWIs Off for This Phone System** check box.

Step 4 Select **Save**.

All MWIs for the phone system are turned off.

Step 5 In the left pane, select **Port**.

Step 6 On the Search Ports page, check the check boxes of the MWI ports that you want to delete.

Step 7 Select **Delete Selected**.

Step 8 In the left pane, select **Phone System**.

Step 9 On the Search Phone Systems page, select the name of the phone system.

Step 10 On the Phone System Basics page, under Message Waiting Indicators, uncheck the **Force All MWIs Off for This Phone System** check box.

Step 11 Select **Save**.

Step 12 To the right of Synchronize All MWIs on This Phone System, select **Run**.

All MWIs for the phone system are synchronized.

To Reconfigure MWI Ports When Port Memory Is Used (PIMG/TIMG Integrations)

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

Step 2 On the Search Phone Systems page, select the name of the phone system.

Step 3 On the Phone System Basics page, under Message Waiting Indicators, check the **Force All MWIs Off for This Phone System** check box.

Step 4 Select **Save**.

All MWIs for the phone system are turned off.

Step 5 In the left pane, select **Port**.

Step 6 On the Search Ports page, select the display name of the first MWI port that you want to reconfigure not to set MWIs.

Step 7 On the Port Basics page, under Port Behavior, enter the applicable settings and select **Save**.

Step 8 If there are more MWI ports that you want to reconfigure not to set MWIs, select **Next**. Otherwise, skip to Step 10.

Step 9 Repeat Step 7 and Step 8 for all remaining MWI ports that you want to configure not to set MWIs.

Step 10 In the left pane, select **Phone System**.

Step 11 On the Search Phone Systems page, select the name of the phone system.

Step 12 On the Phone System Basics page, under Message Waiting Indicators, uncheck the **Force All MWIs Off for This Phone System** check box.

Step 13 Select **Save**.

Step 14 To the right of Synchronize All MWIs on This Phone System, select **Run**.

All MWIs for the phone system are synchronized.

There Is a Delay for MWIs to Turn On or Off

Use the troubleshooting information in this section if there is a delay for MWIs to turn on or off. See the following possible causes:

- If MWIs are being synchronized for a phone system integration, this may result in delayed MWIs for messages. This is due to the additional MWI requests that are being processed.
- The number of ports assigned to handle MWI requests is insufficient. To evaluate the current MWI port activity, see the "Determining the MWI Port Activity" section on page 10-7.

  For systems that handle a large volume of calls, you may need to install additional ports.
- *(Cisco Unified CM SCCP integrations only)* If there are two or more port groups in the phone system integration, the port groups may not all be configured correctly for MWIs. See the "Configuring the MWI On and Off Extensions for Port Groups (SCCP Integrations Only)" section on page 10-7.

Determining the MWI Port Activity

Do the following procedure to generate a report with which you can evaluate the activity of your MWI ports.

To Determine the MWI Port Activity

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Reports**.

Step 2 On the Serviceability Reports page, select **Port Activity Report**.

Step 3 On the Port Activity Report page, select the applicable options for the report.

Step 4 Select **Generate Report**.

Configuring the MWI On and Off Extensions for Port Groups (SCCP Integrations Only)

For Cisco Unified CM SCCP integrations, the phone system integration may have two or more port groups, one of which might be missing the MWI on and off extension settings. Do the following procedure to enter the MWI on and off extensions for all port groups in the SCCP integration.

To Configure the MWI On and Off Extensions for Port Groups (SCCP Integrations Only)

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

Step 2 On the Search Port Groups page, select the name of the first port group for the SCCP integration.

Step 3 On the Port Group Basics page, under Message Waiting Indicator Settings, in the MWI On Extension field, confirm that the extension for turning on MWIs is entered. If the field is blank, enter the MWI On extension.

Step 4 In the MWI Off Extension field, confirm that the extension for turning off MWIs is entered. If the field is blank, enter the MWI Off extension.

Step 5 Select **Save**.

Step 6 Select **Next**.

Step 7 Repeat Step 3 through Step 5 for the remaining port groups in the SCCP integration.

When the MWI Is On, No Message Count Is Given on the Phone

For Cisco Unified CM integrations, Cisco Unity Connection typically provides a message count when the user signs in by phone. If the message count is not given, message counts have not been enabled for new messages or for the type of new message that is in the user voice mailbox. For example, if message counts are enabled only for voice messages, no message count is given when a new email or fax message arrives, even if the MWI is on. To enable message counts for the applicable new messages, do the following procedure.

To Enable Message Counts for the Applicable New Messages

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

Step 2 On the Search Users page, select the alias of the applicable user.

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

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

Step 4 On the Playback Message Settings page, under For New Messages, Play, check the applicable check boxes:

- **Message Count Totals**—Connection announces the total number of messages that are marked new, including voice, email, and fax messages.
- **Voice Message Counts**—Connection announces the total number of voice messages that are marked new.
- **Email Message Counts**—Connection announces the total number of email messages that are marked new.
- **Fax Message Counts**—Connection announces the total number of fax messages that are marked new.
- **Receipt Message Counts**—Connection announces the total number of receipts that are marked new.

Step 5 Select **Save**.

CHAPTER 11

Troubleshooting Audio Quality in Cisco Unity Connection 9.x

See the following sections:

Using the Check Telephony Configuration Test in Cisco Unity Connection 9.x

Note The Check Telephony Configuration test does not test IPv6 connectivity. (IPv6 is supported in Connection for Cisco Unified Communications Manager integrations.) The test confirms that Connection can communicate with the phone system by using IPv4 addressing.

Do the following procedure to use the Check Telephony Configuration test to troubleshoot audio quality.

To Use the Check Telephony Configuration Test

Step 1 In Cisco Unity Connection Administration, in the Related Links box in the upper right corner of any Telephony Integrations page, select **Check Telephony Configuration** and select **Go**.

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

Step 2 In the Task Execution Results window, select **Close**.

Problem with Choppy Audio in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if the audio you hear from Cisco Unity Connection is choppy. Consider the following possible causes:

- The hard disk from which Connection is playing a recording is full. To resolve the situation, eliminate unnecessary files from the hard disk.
- The network connection to the Connection server is not adequate. To resolve the situation, improve the network connection.
- The Connection platform has a malfunctioning component. To resolve the situation, identify the malfunctioning hardware component, then repair or replace it.
- Another process is using too much CPU time. To resolve the situation, stop the process and run it when phone traffic is lighter.

Problem with Garbled Recordings in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if recordings sound garbled. See the following possible scenarios:

- The audio stream sounded garbled when Cisco Unity Connection created the recording. See the "Troubleshooting a Garbled Audio Stream in the Network" section on page 11-2.
- The audio stream did not sound garbled when Cisco Unity Connection created the recording, but became garbled later. See the "Troubleshooting How Cisco Unity Connection Makes Recordings" section on page 11-3.

Troubleshooting a Garbled Audio Stream in the Network

When the audio stream is garbled when Cisco Unity Connection created the recording, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a Garbled Audio Stream in the Network

1. Confirm that the connection to the caller is clear. Calls that have bad PSTN connections or calls from mobile phones may sometimes have garbled audio streams. Connection cannot correct for a garbled audio stream.
2. Determine whether the garbled audio stream is caused by problems with the network. Use network analysis tools to do the following:
   - Check for latency, packet loss, and so on.
   - Search for devices on the network that are causing garbled audio streams. Some examples are routers, gateways, transcoders, and gateways that are configured for one packet size (such as G.711 30ms) while Connection is configured for another packet size (such as G.711 20ms).
3. Determine whether the audio stream is garbled at the closest point to the Connection server by obtaining a sniffer capture at that point. If the audio stream from the sniffer capture is not garbled, Connection may not be handling the audio stream correctly. See the "Troubleshooting How Cisco Unity Connection Makes Recordings" section on page 11-3.

Troubleshooting How Cisco Unity Connection Makes Recordings

When the audio stream did not sound garbled when Cisco Unity Connection created the recording, but became garbled later, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting How Cisco Unity Connection Makes Recordings

1. Enable the Media (Wave) Traces macro traces in Cisco Unity Connection Serviceability. For detailed instructions on enabling the macro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
2. Obtain a snapshot of CPU usage on the Connection server by using the CPU and Memory display in the Real-Time Monitoring Tool (RTMT). For detailed information on using RTMT, see the applicable *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
3. Contact Cisco TAC.

Problem with Garbled Prompts on the Phone in Cisco Unity Connection 9.x

When Cisco Unity Connection prompts sound garbled or jittery when heard on the phone, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Garbled Prompts on the Phone

1. Determine whether the audio stream is garbled at the closest point to the phone by obtaining a sniffer capture at that point. If the audio stream from the sniffer capture is not garbled, the cause may be in the network or with Connection.
2. Determine whether the garbled audio stream is caused by problems with the network. Use network analysis tools to do the following:
   - Check for latency, packet loss, and so on.
   - Search for devices on the network that are causing garbled audio streams. Some examples are routers, gateways, transcoders, and gateways that are configured for one packet size (such as G.711 30ms) while Connection is configured for another packet size (such as G.711 20ms).
3. Determine whether the audio stream is garbled at the closest point to the Connection server by obtaining a sniffer capture at that point. If the audio stream from the sniffer capture is not garbled, Connection may not be handling the audio stream correctly.
4. Enable the Media (Wave) Traces macro traces in Cisco Unity Connection Serviceability. For detailed instructions on enabling the macro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.
5. Obtain a snapshot of CPU usage on the Connection server by using the CPU and Memory display in the Real-Time Monitoring Tool (RTMT). For detailed information on using RTMT, see the applicable *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
6. Contact Cisco TAC.

Problem with the Volume of Recordings in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if the volume of recordings is too loud or too soft, or if the recordings do not have any sound. Consider the following:

- Verify the audio level at each hardware point in the network by obtaining a sniffer capture at each point.
  - If the audio level from the sniffer capture at one point is too soft or too loud, the cause may be the configuration of the hardware (such as routers, gateways, transcoders) at that point. Check the automatic gain control (AGC) settings for the applicable hardware.
  - If the audio level from the sniffer capture at all points is too loud or too soft, see the "Changing the Volume for Cisco Unity Connection Recordings" section on page 11-4.
- Disable automatic gain control (AGC) for Connection so that Connection does not automatically adjust the volume of recordings. See the "Disabling Automatic Gain Control (AGC) for Cisco Unity Connection" section on page 11-4.
- If the recordings do not have any sound, confirm that the advertised codec settings are correct. See the "Confirming the Advertised Codec Settings" section on page 11-5.

Changing the Volume for Cisco Unity Connection Recordings

Do the following procedure.

To Change the Volume for Cisco Unity Connection Recordings

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

Step 2 On the Edit General Configuration page, in the Automatic Gain Control (AGC) Target Decibels field, enter the applicable number.

Note that the AGC decibel levels are set in negative numbers. For example, –26 db is louder than –45 db.

Step 3 Select **Save**.

Disabling Automatic Gain Control (AGC) for Cisco Unity Connection

Do the following procedure.

To Disable Automatic Gain Control (AGC) for Cisco Unity Connection

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

Step 2 On the Search Port Groups page, select the name of the applicable port group.

Step 3 On the Port Group Basics page, on the Edit menu, select **Advanced Settings**.

Step 4 On the Edit Advanced Settings page, under Automatic Gain Control (AGC) Settings, uncheck the **Enable AGC** check box.

Step 5 Select **Save**.

Confirming the Advertised Codec Settings

Do the following procedure.

To Verify the Advertised Codec Settings

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

Step 2 On the Search Port Groups page, select the name of the applicable port group.

Step 3 On the Port Group Basics page, under Advertised Codec Settings, determine whether the list of codecs is correct.

Step 4 If the list is correct, skip to Step 8. Otherwise, select **Change Advertising**.

Step 5 Select the **Up** and **Down** arrows to change the order of the codecs or to move codecs between the Advertised Codec box and the Unadvertised Codecs box.

If only one codec is in the Advertised Codecs box, Connection sends the audio stream in that audio format. If the phone system does not use this audio format, the phone system drops the call.

If two or more codecs are in the Advertised Codecs box, Connection advertises its preference for the first codec in the list but sends the audio stream in the audio format from the list that the phone system selects.

Step 6 Select **Save**.

Step 7 On the Edit menu, select **Port Group Basics**.

Step 8 On the Search Port Groups page, if you want to change the packet size that is used by the advertised codecs, under Advertised Codec Settings, select the applicable packet setting for each codec and select **Save**.

Using Traces to Troubleshoot Audio Quality Issues in Cisco Unity Connection 9.x

You can use traces to troubleshoot audio quality issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

CHAPTER 12

Troubleshooting Licensing in Cisco Unity Connection 9.x

See the following sections:

Troubleshooting Problems with Licenses in Cisco Unity Connection 9.x

When a Cisco Unity Connection feature stops working, when Cisco Unity Connection Administration displays an alert concerning a license violation, or when Connection stops functioning every 24 hours, use the following task list to determine whether the cause is a license violation. We recommend that you do all tasks in the task list to confirm that there are not multiple license violations.

Task List for Troubleshooting Licenses

1. Check if there are unused licensed seats for the applicable Connection feature. To view the licenses that are used currently, see the "Viewing the License Usage in Cisco Unity Connection 9.x" section of the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html. To view the unused licenses on the ELM server, see the "Dashboard view" section of the ELM user guide.
2. Check if Connection is not running in "Expire" mode. See the "Viewing the License Status for Cisco Unity Connection 9.x" section of the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
3. If you need to add a licensed feature when Connection is running in "Expire" mode, see the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Licensing Problems in Cisco Unity Connection 9.x

The following are different licensing problems that may occur in Cisco Unity Connection 9.x and their solutions:

License Violation Status Appears on Cisco Unity Connection Administration

If Connection is registered with the ELM sever and the license violation status is displayed on the Cisco Unity Connection Administration, do the following:

- Confirm that a valid license file for the Cisco Unity Connection features is installed on the ELM server.
- Confirm that the status of the licensed feature on the ELM server is "Compliance" for all the Cisco Unity Connection license tags.

Loss of Connectivity Warning Appears on Cisco Unity Connection Administration for Publisher Server

If the "Loss of Connectivity" warning appears on Cisco Unity Connection Administration for publisher server.

Loss of Connectivity Warning Appears on Cisco Unity Connection Administration for Subscriber Server

If the "Loss of Connectivity" warning appears on Cisco Unity Connection Administration for subscriber server, do the following:

- Check the network connectivity of Cisco Unity Connection on the subscriber server with the ELM server.
- Check the network connectivity of the subscriber server with the Cisco Unity Connection on the publisher server.

Cisco Unity Connection is Not Answering Calls After the License Status Changes from "Expire" to "Compliance"

If Connection is not answering calls after the license status changes from "Expire" to "Compliance", restart the system to resolve the problem.

SpeechView Services are Not Working

If the SpeechView services are not working on Connection, confirm whether the Cisco Unity Connection is configured with the ELM server.

CHAPTER 13

Troubleshooting a Cisco Unity Connection 9.x Cluster Configuration

See the following sections:

Note The Cisco Unity Connection cluster feature is not supported for use with Cisco Unified Communications Manager Business Edition. Requirements for the Connection cluster feature are available in the "Requirements for a Cisco Unity Connection Cluster" section of *System Requirements for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html.

One Server Is Not Functioning and the Remaining Server Does Not Handle Calls in Cisco Unity Connection 9.x

When one Cisco Unity Connection server in a Connection cluster is not functioning (for example, when the subscriber server is undergoing maintenance) and the remaining server does not answer calls or send MWI requests, use the following task list to determine the cause and to resolve the problem.

Task List for Troubleshooting When One Server Is Not Functioning and the Remaining Server Does Not Handle Calls

1. Verify the status of the voice messaging ports in Cisco Unity Connection Serviceability. See the "Verifying the Status of the Voice Messaging Ports in Cisco Unity Connection Serviceability" section on page 13-2.

2. Verify the voice messaging port assignments for the phone system integration. See the "Verifying the Voice Messaging Ports Assignments for the Phone System Integration" section on page 13-2.
3. For SCCP integrations, confirm that the voice messaging ports are registered with the Cisco Unified CM server. See the "Confirming That the Voice Messaging Ports Are Registered (SCCP Integrations Only)" section on page 13-3.
4. Enable the SRM micro trace (all levels) in Cisco Unity Connection Serviceability. For detailed instructions on enabling the micro trace and viewing the trace logs, see the "Using Cisco Unity Connection Serviceability Traces to Troubleshoot Problems" section on page 2-9.

Verifying the Status of the Voice Messaging Ports in Cisco Unity Connection Serviceability

Do the following procedure.

To Verify the Status of the Voice Messaging Ports in Cisco Unity Connection Serviceability

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Cluster Management**.

Step 2 On the Cluster Management page under Port Manager, verify the following for the server that should be handling calls:

- In the Total Ports column, the number of ports that is listed is correct.
- In the Change Port Status column, the Stop Taking Calls button appears. If the Take Calls button appears, select **Take Calls**.

Verifying the Voice Messaging Ports Assignments for the Phone System Integration

Do the following procedure.

To Verify the Voice Messaging Port Assignments for the Phone System Integration

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

Step 2 In the Related Links list, select **Check Telephony Integration** and select **Go**.

The Task Execution Results displays one or more messages with troubleshooting steps.

Step 3 Follow the steps for correcting the problems.

Step 4 Repeat Step 2 through Step 3 until the Task Execution Results displays no problems.

Confirming That the Voice Messaging Ports Are Registered (SCCP Integrations Only)

For Cisco Unified CM SCCP integrations, do the following procedure.

To Confirm That the Voice Messaging Ports Are Registered (SCCP Integrations Only)

Step 1 In Cisco Unified CM Administration, on the Voice Mail menu, select **Voice Mail Port**.

Step 2 On the Find and List Voice Mail Ports page, select **Find**.

Step 3 In the Status column, confirm that all ports show the status of "**Registered with <server name>**."

Both Servers Have Primary Server Status in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if both servers in the Cisco Unity Connection cluster have Primary server status (a "split brain" condition). See the following possible causes:

- The network is not functioning or is preventing the publisher and subscriber servers from communicating with each other.

  The solution is to restore the network connection so that the publisher and subscriber servers can communicate.

- The host name for the subscriber server was changed and is not entered correctly on the System Settings > Cluster page of the publisher server.

  The solution is to enter the correct host name of the subscriber server on the System Settings > Cluster page of the publisher server.

After the Subscriber Server is Reinstalled, the Cluster Status is Not Updated on both the Publisher and Subscriber Servers

Use the troubleshooting information in this section if the cluster status is not updated on both the servers in Connection 8.x cluster. See the following possible issues:

- The subscriber server fails to be added to the cluster in Unity Connection 8.x even after it has been successfully reinstalled. The cluster status on subscriber server that is displayed by the CLI command show cuc cluster status, returns an error as:

Incorrect password or user com.informix.asf.IfxASFRemoteException: cucli@servername is not known on the database server

- The cluster status on publisher server that is displayed by the CLI command show cuc cluster status, returns an error as:

<The publisher as single server>

Database replication is not active.

Follow the given steps to resolve this issue:

- Contact TAC for assistance. The TAC engineer must take the root access of the publisher server and tear down the replication between publisher and subscriber server.
- Rebuild the subscriber server after this to resolve the issue.

Cisco Unity Connection 9.x Cluster Is Not Functioning Correctly

When a Cisco Unity Connection cluster is not functioning correctly (for example, server status does not change when expected), use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting a Cisco Unity Connection Cluster That Is Not Functioning Correctly

1. Confirm that the applicable services are running on the server with primary server status. See the "Confirming That the Applicable Services Are Running on the Server with Primary Server Status" section on page 13-4.
2. Confirm that the applicable services are running on both servers. See the "Confirming That the Applicable Services Are Running on Both Servers" section on page 13-4.
3. Use traces to troubleshoot the Connection cluster. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Traces in Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x" section on page 2-1.

Confirming That the Applicable Services Are Running on the Server with Primary Server Status

Do the following procedure.

To Confirm That the Applicable Services Are Running on the Server with Primary Server Status

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 On the Control Center - Feature Services page, under Critical Services, confirm that the following services have the **Started** service status:

- Connection Message Transfer Agent
- Connection Notifier

Step 3 If the services have the **Stopped** service status, select **Start**.

Confirming That the Applicable Services Are Running on Both Servers

Do the following procedure.

To Confirm That the Applicable Services Are Running on Both Servers

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 On the Control Center - Feature Services page, under Status Only Services, confirm that the Connection Server Role Manager service has the **Started** service status.

The services in the Status Only Services section cannot be started in Cisco Unity Connection Serviceability. You must use the command line interface (CLI) to start or stop these services. For information on the CLI, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 9.0(1)* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 3 Under Critical Services, check the service status for the following services:

- Connection Conversation Manager
- Connection Mixer

If the services have the **Started** service status, skip to Step 4. If the services have the **Stopped** service status, select **Start**.

Step 4 Under Base Services, check the service status for the Connection DB Event Publisher service.

If the service has the **Started** service status, skip to Step 5. If the service has the **Stopped** service status, select **Start**.

Step 5 Under Optional Services, check the service status for the following services:

- Connection File Syncer
- Connection IMAP Server
- Connection SMTP Server

If the service has the **Stopped** service status, select **Start**.

Server Cannot Be Added to the Cisco Unity Connection 9.x Cluster

Use the troubleshooting information in this section if the Add New button is disabled on the System Settings > Cluster page so that you cannot add a server to the Cisco Unity Connection cluster. See the following possible reasons why the Connection cluster feature is not available:

- Connection is installed as Cisco Unified Communications Manager Business Edition (CMBE), which does not support the Connection cluster feature. See the "Requirements for a Cisco Unity Connection Cluster" section of *System Requirements for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html .
- The size of the hard disc on the publisher server is inadequate for supporting the Connection cluster feature. Both servers in a Connection cluster must meet the specifications in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.
- The number of servers in the Connection cluster is the maximum that is supported. No more servers can be added to the Connection cluster. For information on replacing Connection servers in a Connection cluster, see the "Replacing Cisco Unity Connection 9.x Servers" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrugx.html.

Cannot Access Alert Logs When the Publisher Server Is Not Functioning in Cisco Unity Connection 9.x

When the publisher server is not functioning and you cannot access the alert logs from the subscriber server, you must specify the subscriber server as the failover collector. Do the following procedure.

To Enable the Subscriber Server to Access the Alert Logs When the Publisher Server Is Not Functioning

Step 1 On the publisher server, in Cisco Unity Connection Administration, expand **System Settings**, then select **Service Parameters**.

Step 2 On the Service Parameters page, in the Server field, select the publisher server.

Step 3 In the Service field, select **Cisco AMC Service**.

Step 4 In the Failover Collector field, select the subscriber server.

Step 5 Select **Save**.

Step 6 In the navigation list, select **Cisco Unified Serviceability** and select **Go**.

Step 7 In Cisco Unified Serviceability, in the Tools menu, select **Control Center - Network Services**.

Step 8 In the Server field, select the subscriber server and select **Go**.

Step 9 Under Performance and Monitoring, select **Cisco AMC Service** and select **Restart**.

Step 10 When prompted to confirm that you want to restart the service, select **OK**.

CHAPTER 14

Troubleshooting User and Administrator Access in Cisco Unity Connection 9.x

See the following sections for information on problems that can occur when users and administrators access Cisco Unity Connection:

Cisco Unity Connection 9.x Does Not Respond to Key Presses

When Cisco Unity Connection is integrated by SCCP to Cisco Unified Communications Manager, Cisco Unity Connection may not respond to key presses.

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 Connection, use the following command:

dtmf-relay h245-alphanumeric

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

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

Users Do Not Hear Sign-in Prompt When Calling Cisco Unity Connection 9.x

When a user calls Cisco Unity Connection directly and unexpectedly hears the Opening Greeting or another prompt rather than the sign-in prompt, the problem can be caused by either of the following:

- The call matched a direct call routing rule other than the Attempt Sign-In rule, and the rule directed the call to a destination other than the Attempt Sign-In conversation.
- The calling extension is not found in the search scope set by the call routing rule that sent the call to the Attempt Sign-In conversation.

Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is attempting to sign in. If the user extension is in a partition that is not a member of the search space that is assigned as the search scope of the call by the routing rule, Connection routes the call to the Opening Greeting.

To resolve this problem, in Cisco Unity Connection Administration, check the direct call routing rules to determine which rule is processing the call and to check the search scope that is set by the rule. You can also enable the Arbiter micro trace (levels 14, 15, and 16 call routing), the RoutingRules micro trace (level 11 rules creation/deletion/evaluation) and the CDE micro trace (level 4 search space). (For detailed instructions on turning on traces and collecting logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Users Cannot Access Cisco Personal Communications Assistant Pages in Cisco Unity Connection 9.x

Users use the Cisco Personal Communications Assistant (PCA) website to access the Messaging Assistant, and the Cisco Unity Connection Personal Call Transfer Rules pages.

When a user cannot access the Cisco PCA pages, consider the following possible causes.

- **The Cisco PCA URL is case-sensitive**—Users can access the Cisco PCA at the following URL: http://<Cisco Unity Connection server>/ciscopca. Note, however, that the URL is case-sensitive.
- **The browser or client configuration is not configured properly**—When a user cannot access any of the Cisco PCA pages, it may be that the user browser or client workstation is not configured properly. Make sure that the browser and client workstation are configured as specified in the *User Workstation Setup Guide for Cisco Unity Connection Release 9.x*. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.
- **Unsupported software is installed on the client workstation**—Confirm that the user does not have an unsupported combination of software or an unsupported third-party application installed on the workstation. See the *Compatibility Matrix: Cisco Unity Connection and the Software on User*

Workstations, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html.

Additional troubleshooting information and procedures for the Cisco PCA are available in the "Troubleshooting the Cisco Personal Communications Assistant (PCA) in Cisco Unity Connection 9.x" chapter.

Also note that the users can access the Web Inbox URL, and link to the Messaging Assistant and Cisco Unity Connection Personal Call Transfer Rules pages from there. The Web Inbox URL is http://<Connection server>/inbox.

Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages in Cisco Unity Connection 9.x

If you use the self-signed certificate generated during installation to provide an SSL connection to the Cisco PCA, the web browser of the user displays a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Similarly, if you use a self-signed SSL certificate to secure IMAP email client access to Connection, some email clients supported for use with Connection display SSL security messages.

Although users can still access Connection despite the alerts, consider one of the following options to manage or eliminate security alerts when users browse to Cisco PCA and/or access their messages from an IMAP email client:

- Add the SSL certificate to the Trusted Root Store on each user workstation. In this way, you can ensure that users never see the security alert. See the following "To Add the SSL Certificate to the Trusted Root Store on User Workstations" procedure.
- Tell users to select the "Accept Permanently" (or similar) option when the browser or email client displays the alert and asks them how to proceed. After instructing the browser and/or email client to always accept the certificate, the user will not see the alert again.

Do the following procedure if you want users to never see the security alert.

To Add the SSL Certificate to the Trusted Root Store on User Workstations

Step 1 From the OS Administration application on the Cisco Unity Connection server, right-click to download the certificate and save it as a file.

Step 2 Copy the certificate to each user workstation, and then import it by using tools in the browser or IMAP client, as applicable.

Users Cannot Access the Connection Web Tools from the Cisco PCA in Cisco Unity Connection 9.x

When users can access the Cisco Personal Communications Assistant (PCA), but cannot access the Messaging Assistant, or the Cisco Unity Connection Personal Call Transfer Rules, consider the following possible causes:

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

Note Web Inbox has replaced the Messaging Inbox. See the "Troubleshooting the Web Inbox in Cisco Unity Connection" chapter for Web Inbox troubleshooting information.

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

Users Cannot Save Changes on Pages in the Cisco PCA in Cisco Unity Connection 9.x

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

Administration Accounts Cannot Sign In to Cisco Unified Serviceability When the Default Application Administration Account Is Locked

When the default application administration account is locked, for example, because the password has expired or because of too many unsuccessful sign in attempts, no application administration account is allowed to sign in to Cisco Unified Serviceability. (You specify the account name and password for the default application administration account during installation, and you create and administer additional application administration accounts in Cisco Unity Connection Administration.)

To unlock the account, change the password by using the **utils cuc reset password** CLI command. Changing the password also unlocks the account. (If an account has been hacked, you do not want to unlock it without also changing the password.)

"Access Denied" Error is Displayed on Cisco Unity Connection Administration

If you receive "Access Denied" error on the Cisco Unity Connection Administration, make sure that you have not used the keywords (update, delete, insert, and union) along with some other characters at the end in the display name of an object. For example, if you enter "updateschedule" in the display name of a Schedule, it will throw "Access Denied" error. To resolve this issue, remove "schedule" from the display name.

CHAPTER 15

Troubleshooting Call Transfers and Call Forwarding in Cisco Unity Connection 9.x

See the following sections:

Note For call transfer problems that occur on newly installed systems, see the applicable Cisco Unity Connection integration guide, at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

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 in Cisco Unity Connection 9.x

When calls are not transferred to the correct greeting, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Call Transfers to the Wrong Greeting

1. Confirm that the forward timer in the phone system is synchronized with the Rings to Wait For setting in Cisco Unity Connection. See the "Confirming That the Forward Timer in the Phone System Is in Synch with the Rings to Wait For Setting in Cisco Unity Connection" section on page 15-2.
2. Confirm that the phone system programming enables callers to hear the personal greeting of the user. See the "Confirming That the Phone System Integration Enables Playing the User Personal Greeting for Callers" section on page 15-3.
3. Confirm that the busy greeting is supported and enabled. See the "Confirming That the Busy Greeting Is Supported and Enabled" section on page 15-4.

4. Confirm that the caller reaches the intended destination based on the search scope. See the "Confirming That the Search Scope Configuration Sends the Call to the Intended Destination" section on page 15-4.

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

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

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

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

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

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

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

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

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

Step 4 On the Edit User Basics page, on the Edit menu, select **Transfer Rules**.

Step 5 On the Transfer Rules page, select the name of the active transfer rule.

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

Step 7 In the Transfer Type list, confirm that **Supervise Transfer** is selected.

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

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

Step 9 Select **Save**.

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

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

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

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

Step 12 On the Edit User Template Basics page, on the Edit menu, select **Transfer Rules**.

Step 13 On the Transfer Rules page, select the name of the active transfer rule.

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

Step 15 In the Transfer Type list, confirm that **Supervise Transfer** is selected.

Step 16 In the Rings to Wait For field, enter the same setting that you entered in Step 8.

Step 17 Select **Save**.

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

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

To Verify the Phone System Integration Settings

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

Step 2 Confirm that the settings for the phone system, port group, and ports match those indicated in the applicable Cisco Unity Connection integration guide, at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

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

Step 4 Confirm that the extension that the caller reached is the same as the primary or alternate extension of the user.

Step 5 If callers still hear the opening greeting after dialing the user extension, contact Cisco TAC.

Confirming That the Busy Greeting Is Supported and Enabled

When a call arrives at a busy extension and is forwarded to Cisco Unity Connection, phone systems typically send the reason for forwarding (the extension is busy) along with the call.

If Connection does not play the user busy greeting for the caller, the cause may be one of the following:

- The phone system does not provide the necessary call information to support the busy greeting. See the "Integration Functionality" section in the applicable Cisco Unity Connection integration guide, at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
- The user has not enabled the busy greeting. See the *User Guide for the Cisco Unity Connection Phone Interface (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucugphone.html or the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.
- The alternate greeting for the user is enabled and overrides the busy greeting. See the *User Guide for the Cisco Unity Connection Phone Interface (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucugphone.html or the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.

Confirming That the Search Scope Configuration Sends the Call to the Intended Destination

If a caller enters digits to transfer to an extension from the automated attendant or from a user greeting and reaches an unintended destination, check the search scope of the call at the point where the caller enters the digits. Cisco Unity Connection uses the search scope to match the extension that the caller dials to an object with this extension, such as a user, contact, or remote contact at a VPIM location. In particular, if your dial plan includes overlapping extensions, it is possible for the caller to enter an extension that matches multiple users or other Connection objects and be transferred to a different object than the caller expects to reach.

To make a match by extension, Connection checks the search space that is currently defined as the search scope for the call. Connection searches the partitions in this search space in the order that they appear in the Assigned Partitions list in Cisco Unity Connection Administration, and returns the first result found.

The search scope of the call when the caller reaches a system call handler is defined by the Search Scope setting on the Call Handler Basics page for the handler, and may either be explicitly set to a particular search space, or may be set to inherit the search space from the call, in which case it may have been set by a previous handler or by the last call routing rule that processed the call. When a user greeting is played, the search scope of the call is defined by the Search Scope setting on the User Basics page for the user in Cisco Unity Connection Administration.

You can trace the search scope of a call by enabling the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Problems with Call Transfers in Cisco Unity Connection 9.x (Cisco Unified Communications Manager Express SCCP Integrations Only)

For Cisco Unified Communications Manager Express SCCP integrations only, call transfers may not work correctly (for example, the call may be dropped or the caller may be left on hold indefinitely). A possible cause for this problem is that the phone system integration is not correctly configured for Cisco Unified Communications Manager Express.

Do the following procedure.

To Configure the SCCP Integration for Cisco Unified Communications Manager Express

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

Step 2 On the Search Port Groups page, select the port group name that is used by the Cisco Unified CM Express SCCP integration.

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

Step 4 Under Cisco Unified Communications Manager Servers, in the Server Type column, select **Cisco Unified Communications Manager Express** and select **Save**.

User Hears a Reorder Tone When Answering a Notification Call from Cisco Unity Connection 9.x

Cisco Unity Connection requires a minimum Rings to Wait For setting of three rings 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 for notification devices or call handlers, a user may hear the reorder tone instead of the Connection conversation when called by Connection.

To Correct the Rings to Wait For Setting

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

Step 2 On the Search Users page, select the alias of the user who is hearing a reorder tone when answering a call from Connection.

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

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

Step 4 On the Notification Devices page, select the display name of a notification device.

Step 5 On the Edit Notification Device page, under Phone Settings, set the Rings to Wait field to three or more rings.

Step 6 Select **Save**.

Step 7 On the User menu, select **Notification Devices**.

Step 8 Repeat Step 4 through Step 7 for each remaining notification device.

Step 9 To change the default Rings To Wait value for future users, expand **Templates** and select **User Templates**.

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

Step 10 On the Search User Templates page, select the alias of the user template that you want to change.

Step 11 On the Edit User Template Basics page, on the Edit menu, select **Notification Devices**.

Step 12 On the Notification Devices page, select the display name of a notification device.

Step 13 On the Edit Notification Device page, under Phone Settings, set the Rings to Wait field to three or more rings.

Step 14 Select **Save**.

Step 15 On the User menu, select **Notification Devices**.

Step 16 Repeat Step 12 through Step 15 for each remaining notification device.

Step 17 Expand **Call Management**, then select **System Call Handlers**.

Step 18 On the Search Call Handlers page, select the display name of a call handler.

Step 19 On the Edit Call Handler Basics page, on the Edit menu, select **Transfer Rules**.

Step 20 View the Standard, Alternate, and Closed rules. In the Transfer Type field, 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 user still hears a reorder tone when answering a call from Connection, contact Cisco TAC.

CHAPTER 16

Troubleshooting Messages in Cisco Unity Connection 9.x

See the following sections:

Message Quota Enforcement: Responding to Full Mailbox Warnings in Cisco Unity Connection 9.x

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

- If a mailbox has reached the size of the warning quota, the user hears a warning that the mailbox is almost full.
- If a mailbox has reached the size of the send quota, the user is unable to send messages and hears a warning that messages cannot be sent. If the user mailbox contains deleted messages, Cisco Unity Connection offers the option to remove all deleted messages.
- If a mailbox has reached the size of the send/receive quota:
  - The user is unable to send messages.
  - The user hears a warning that messages cannot be sent.
  - Unidentified callers are not allowed to leave messages for the user.
  - Messages from other users generate nondelivery receipts to the senders.
  - If the user mailbox contains deleted messages, Connection offers the option to remove all deleted messages. If necessary, the user can also remove saved or new messages individually until the mailbox size is below the quotas.

Troubleshooting Undeliverable Messages in Cisco Unity Connection 9.x

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

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

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

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

However, if the original message is malformed, rather than sending the message to the Undeliverable Messages list, Connection places the message in the MTA bad mail folder (UmssMtaBadMail). This folder is automatically checked nightly by the Monitor Bad Mail Folders task, and if messages are found, an error is written to the application event log indicating troubleshooting steps.

Messages Appear to Be Delayed in Cisco Unity Connection 9.x

Use the following task list to troubleshoot the possible causes for the apparent delay of messages.

Task List for Troubleshooting Delay in Appearance of Messages

1. To verify the arrival times of messages, generate a user message activity report for the user. For more information, see the "Generating and Viewing Reports in Version 9.x" section in the "Using Reports in Version 9.x" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.
2. See the applicable information in the "Orientation Task List for Cisco Unity Connection 9.x Users" section in the "User Orientation in Cisco Unity Connection 9.x" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Some Messages Seem to Disappear in Cisco Unity Connection 9.x

See the following troubleshooting steps for investigating messages that are not being delivered to the intended recipients.

- Confirm that users who are assigned to the Undeliverable Messages distribution list have been forwarding messages to the intended recipients. See the "Undeliverable Messages Have Not Been Forwarded to Recipients" section on page 16-4.
- Confirm that the user mailbox is not full. See the "User Has a Full Mailbox" section on page 16-3.
- Confirm that you or another administrator did not inadvertently delete a user who was assigned to review the messages for Cisco Unity Connection entities. See the "Users Assigned to Cisco Unity Connection Entities Were Deleted and No Replacements Were Assigned" section on page 16-4.
- Review message aging settings. See the "Changing a Message Aging Policy" section in the "Controlling the Size of Mailboxes in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The message may have been flagged for dispatch delivery. When users are members of a distribution list that is the recipient of a call handler that is configured to mark messages for dispatch delivery, it is possible for the users to receive a message, but then later find that the message has been removed from their mailboxes because another member of the distribution list accepted the message. See the "Dispatch Messages in Cisco Unity Connection 9.x" section in the "Messaging in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The user account may be configured to relay one or more message types to another SMTP address, but the message relay is failing. See the "Cisco Unity Connection Is Unable to Relay Messages" section on page 16-5.

User Has a Full Mailbox

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

- By default, when an unidentified caller attempts to send a message to a user whose mailbox has exceeded the send/receive quota, Connection still delivers the message. You can instead configure Connection to indicate to the caller that the recipient mailbox is full, and prevent the caller from recording a message for that recipient. (In Cisco Unity Connection Administration, on the Message Storage > Mailbox Quotas page, check the Full Mailbox Check for Outside Caller Messages check box.)

  If the recipient mailbox has not yet exceeded the send/receive quota at the time an unidentified caller records a message, but the quota is exceeded in the act of delivering the message, Connection delivers the message regardless of the quota.
- When a user tries to leave a message for another user whose mailbox has exceeded the send/receive quota, Connection allows the user to record and send the message. However, if the mailbox for the recipient is full, he or she does not receive the message, and if the user account for the recipient is configured to send non-delivery receipts when message delivery fails, Connection sends the message sender a non-delivery receipt.

  If the recipient mailbox has not yet exceeded the send/receive quota at the time a Connection user records a message, but the quota is exceeded in the act of delivering the message, Connection delivers the message regardless of the quota.

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

Read receipts and non-delivery receipts are sent and delivered regardless of the status of the mailbox quota.

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

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

Undeliverable Messages Have Not Been Forwarded to Recipients

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

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

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

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

- Undeliverable Messages distribution list (by default, the UndeliverableMessagesMailbox user account is the only member of this distribution list)
- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

Cisco Unity Connection Is Unable to Relay Messages

Cisco Unity Connection uses the settings on the Message Actions page for a user in Cisco Unity Connection Administration to determine how to handle the different types of messages that it receives for the user. The relay action instructs Connection to send all messages of a certain type to a relay address on a different messaging system (such as a corporate email server) for storage and user access.

If the relay address that is configured for a user matches one of the user SMTP proxy addresses that is configured on the system, Connection does not relay messages to the relay address, to avoid possible delivery loops. If Connection were to relay a message to a proxy address, it is possible that the proxy address would resolve back to the same Connection mailbox that relayed the original message, thus creating an infinite loop.

When configuring relay addresses for message relay, we recommend that you use the precise email address of the destination mailbox, for example, alias@mailserver.

Message Audio Cannot Be Played in Outlook Web Access

When Cisco Unity Connection is configured to relay messages to a Microsoft Exchange server (by using the Relay the Message or the Accept and Relay the Message action), users who use Outlook Web Access to access their Exchange mailboxes may not be able to play the message audio. When this occurs, the message header indicates that the audio attachment is available for the message, but the user cannot view or play the attachment when the message is opened. For a resolution to this issue in Microsoft Exchange 2007, refer to Microsoft Knowledge Base article 954684.

Troubleshooting Recorded Messages Not Being Allowed to Exceed 30 Seconds in Length in Cisco Unity Connection 9.x

If recorded voice messages are not being allowed to exceed 30 seconds, confirm that the Cisco Unity Connection license file has the LicMaxMsgRecLenIsLicensed license tag enabled. Do the following procedure.

To Confirm That the LicMaxMsgRecLenIsLicensed License Tag Is Enabled in the License File

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

Step 2 On the Licenses page, under License Count, confirm that the value of Voice Message Recordings Longer Than 30 Seconds Allowed (LicMaxMsgRecLenIsLicensed) is set to **Yes**.

CHAPTER 17

Troubleshooting IMAP Clients and ViewMail for Outlook in Cisco Unity Connection 9.x

See the following sections for problems that can occur in IMAP clients and in Cisco Unity Connection ViewMail for Microsoft Outlook:

Troubleshooting Problems with Changing Passwords in Cisco Unity Connection 9.x

When users change their Cisco Personal Communications Assistant (PCA) password in the Messaging Assistant, they also must update the password from their IMAP email client application so that the client can continue to access Connection and retrieve voice messages. Likewise, when LDAP authentication is configured and the PCA password is changed in LDAP, the password configured in the IMAP email client application must be updated.

Users who use ViewMail for Outlook also must change the password in ViewMail for Outlook options when the PCA password has been changed. If the PCA password has been changed but ViewMail has not been updated, users typically see a message indicating that the invalid credentials were entered for the account when they try to use ViewMail features.

Troubleshooting Sign-In Problems with IMAP Email Clients in Cisco Unity Connection 9.x (When LDAP Is Not Configured)

If users have trouble signing in to an IMAP client, or have trouble receiving voice messages in an IMAP client, consider the following possibilities:

- If the IMAP client application prompts a user for the Cisco Personal Communications Assistant (PCA) password, but does not accept it:
  - The Cisco Unity Connection user account may be locked because of too many invalid sign-in attempts.
  - The Connection user account may have been locked by an administrator.
  - The Connection user password may have expired.
  - The Connection user account may have been configured to require that the user specify a new password.
  - The Connection user may be entering the wrong password.

  Users who belong to a class of service that allows access to the Messaging Assistant or to the Messaging Inbox can try to sign in to the Cisco PCA instead; the Cisco PCA displays an error message that explains why the sign-in attempt is failing. Users who cannot access the Messaging Assistant or the Messaging Inbox must contact an administrator for assistance.
- If Microsoft Outlook users are not prompted for their Cisco PCA password, confirm that the Remember Password check box on the Internet Email Settings (IMAP) page is not checked. If this option is checked, and the password of the user has expired, changed, or is locked, Microsoft Outlook does not prompt the user to enter the Cisco PCA password. The result is that the user does not receive voice messages from Connection, and Outlook prompts for the username and password.

Troubleshooting Sign-In Problems with IMAP Email Clients in Cisco Unity Connection 9.x (When LDAP Is Configured)

If you are using LDAP authentication and using an IMAP email client to access Cisco Unity Connection voice messages, and if users who are integrated are with the LDAP are unable to authenticate, consider the following possibilities:

- If you are using Active Directory, confirm that the server you are using for authentication is a global catalog server and that you are using port 3268 (if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Connection server) or port 3269 (if you are using SSL). Authentication settings are on the System Settings > LDAP > LDAP Authentication page in Connection Administration.

  If you change any values on the LDAP Authentication page, and if IMAP clients are accessing Connection, restart the Connection IMAP Server service in Cisco Unity Connection Serviceability. If other web applications are accessing Connection (for example, Cisco Personal Communications Assistant), restart the server.

- If the problem occurs even though you are already using a global catalog server or you are not using Active Directory, try to sign in to the Cisco PCA by using an account that cannot sign in to an IMAP email client.
  - If that fails, then there are two likely causes: either the specifications on the LDAP Authentication page are incorrect, or there is a problem with user credentials on the LDAP server, for example, the password has expired or the user is specifying the wrong password.
  - If that succeeds, and if you have configured SSL to encrypt data that is transmitted between the LDAP server and the Connection server, there may be a problem with the SSL certificate. To confirm, uncheck the Use SSL check box, change the port to 3268, restart the Connection IMAP Server service in Cisco Unity Connection Serviceability, and try again.

Messages Sent From an IMAP Client Are Not Received in Cisco Unity Connection 9.x

If users cannot send messages through the Cisco Unity Connection server from an IMAP client—for example, messages remain in the Outbox, an SMTP error is displayed in the client, or users receive non-delivery receipts (NDRs)—consider the following possibilities:

- If Connection is not configured to allow clients to connect from untrusted IP addresses on the System Settings > SMTP Configuration > Server page in Cisco Unity Connection Administration, the IP address of the client must appear in the IP address access list in Connection. See the "Checking the IP Address Access List" section on page 17-4.
- If Connection is configured to allow clients to connect from untrusted IP addresses on the System Settings > SMTP Configuration > Server page in Connection Administration, two additional settings on this page can affect the ability of an IMAP client to send messages.
  - If the Require Authentication From Untrusted IP Addresses check box is checked, the client must be configured to authenticate with the outgoing SMTP server.
  - If the Transport Layer Security From Untrusted IP Addresses field is set to Required, the client must be configured to use Secure Sockets Layer (SSL) when connecting to the Connection server.

- The email address of the message sender must exactly match a primary or proxy SMTP address configured in Connection, as follows:
  - If the message is being sent from an IMAP client that is authenticated with the Connection server, the email address must exactly match either the primary SMTP address that is displayed on the User Basics page for the user in Connection Administration or one of the SMTP proxy addresses that are configured on the SMTP Proxy Addresses page for the user.
  - If the message is being sent from an IMAP client that is not authenticated with the Connection server, the email address can match a primary or proxy address that is configured for any user on the Connection server.
- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found, Connection relays the message to the SMTP smart host, or sends an NDR to the sender, depending on the option selected in the When a Recipient Cannot be Found setting on the System Settings > General Configuration page in Connection Administration. By default, Connection sends an NDR.
- The message exceeds the maximum length or number of recipients per message that are configured on the System Settings > SMTP Server Configuration page in Connection Administration. (By default, the maximum allowed message length is 10 MB.)
- The IMAP client is unable to reach the Connection SMTP server because of network connectivity issues or because access is blocked by a firewall.

In many of these error cases, the IMAP client may display an SMTP error when attempting to send a message to the Connection server. This error includes an error code and a text description that can help narrow down the source of the problem. If the client application does not display SMTP errors to the user, or if you still have not identified the problem after checking the potential causes above, the SMTP and MTA micro traces (all levels) are helpful for diagnosing issues related to SMTP connectivity and message transport. When examining the logs, start with the SMTP log first, then review the MTA log. (The SMTP service authenticates the client and receives the message; the MTA service processes the message and addresses it to the correct Connection user or contact.) For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Checking the IP Address Access List

If you choose not to allow connections from untrusted IP address lists, the IP address of each client must be configured in the IP access list, and the Allow Connection check box must be checked. If the access list is not configured properly, the client may display an SMTP error code of 5.5.0, indicating that the connection was refused. Do the following procedure to check and update the IP address access list.

To Check the Cisco Unity Connection IP Address Access List

Step 1 In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Server**.

Step 2 On the SMTP Configuration Page, on the Edit menu, select **Search IP Address Access List**.

Step 3 Confirm that the IP address in use by the IMAP client appears as an entry in the list, and that the Allow Connection check box is checked.

Step 4 To add a new IP address to the list, select **Add New**.

Step 5 On the New Access IP Address page, enter an IP address, or you can enter a single * (asterisk) to match all possible IP addresses.

Step 6 Select **Save**.

Step 7 On the Access IP Address page, check the **Allow Connection** check box to allow connections from the IP address that you entered in Step 4. To reject connections from this IP address, uncheck the check box.

Step 8 If you have made any changes on the Access IP Address page, select **Save**.

Messages Are Received in an Email Account Rather Than a Voice Mailbox in Cisco Unity Connection 9.x

If users unexpectedly receive voice messages in their corporate or other email accounts rather than their Cisco Unity Connection mailboxes, consider the following possibilities:

- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found and Connection is configured to relay the message to the SMTP smart host, the message is relayed to the applicable email address. Confirm that the message recipient has a proxy SMTP address configured for the applicable email address. See the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
- If the user email profile has an Exchange account, the Cached Exchange Mode setting in Outlook must be enabled.
- If message actions for the recipient are configured to relay messages of a particular type (voice, email, fax or delivery receipt) to the user at the corporate email address, this is the expected behavior.

Voice Messages Are Not Received in an IMAP Account

If users do not receive incoming voice messages in the email client inbox, check the Junk-Email or other spam folder. The mail client may automatically filter voice messages to this folder. For information on configuring spam filtering to exclude a class of messages, refer to the email client documentation.

You may also need to check the configuration of any email appliance or server-side anti-spam filters in your organization to see if voice messages are being routed to Junk mail, voice attachments are being removed, or the policy is otherwise interfering with the delivery of voice messages to user mail clients.

Intermittent Message Corruption When Using Cisco Unity Connection ViewMail for Microsoft Outlook 8.0

In cases where user email profiles have an Exchange account, and the users are using Cisco Unity Connection ViewMail for Microsoft Outlook 8.0, they may experience the following intermittent problems:

- When using ViewMail for Outlook to reply to a voice message, the recipient receives a corrupt voice message that cannot be played.
- When using ViewMail for Outlook to forward a voice message with an introduction to another Connection user, the recipient hears only the introduction; the original message is not heard.
- When using ViewMail for Outlook to forward a voice message to another Connection user, the message is delivered to the Exchange mailbox of the recipient instead of to the Connection mailbox of the recipient. Additionally, the message is corrupt, and cannot be played.

For each of these problems, the solution is to enable the Cached Exchange Mode setting in Outlook.

Recording or Playback Devices Do Not Appear in ViewMail Account Settings in Cisco ViewMail for Microsoft Outlook

If a particular recording or playback device that is connected to the computer does not appear as an option in the Audio Devices lists while composing a message or in the ViewMail Account Settings dialog, restart Outlook. ViewMail for Outlook does not recognize devices that were recently added to the computer until you restart Outlook.

Messages Cannot Be Played through Cisco ViewMail for Microsoft Outlook 8.5 and Later

If the "Recording or Playback Messages Failed - no recording device" error message appears while recording or playing voice messages through ViewMail for Outlook 8.5 and later, make sure that the proxy is not enabled in the Internet Explorer. If you want to play or record voice messages while proxy is enabled, you need to add the hostname or IP address of Cisco Unity Connection in the proxy exception list to avoid failure in recording or playing voice messages through ViewMail.

User Email Account Does Not Appear in ViewMail Options in Cisco ViewMail for Microsoft Outlook

If you have recently added an email account to Outlook but the account does not appear as an option when you try to add it as an Associated Email Account in ViewMail Options, restart Outlook. ViewMail for Outlook does not recognize email accounts that were recently added to Outlook until you restart Outlook.

Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 Form Does Not Appear

If the Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 form does not appear after you have installed ViewMail on a user workstation, consider the following:

- Only new messages are displayed with the form. Messages that were in the user mailbox prior to installing ViewMail do not display with the form.
- You must close and restart Outlook after installing ViewMail. If the user is running a synchronization program for a PDA device, the Outlook.exe process may not have fully exited when Outlook was shut down. If that is the case, close the synchronization program and then close and restart Outlook.
- The ViewMail form may have been disabled by Outlook. To determine if Outlook has disabled the form, select Help > About Microsoft Office Outlook > Disabled Items to see whether vmoexchangeextension.dll is in the list.

Using Diagnostic Traces for IMAP Client Problems in Cisco Unity Connection 9.x

See the following sections:

- Collecting Diagnostics from ViewMail for Outlook on the User Workstation, page 17-7
- Collecting Diagnostics from ViewMail for Outlook 8.0 on the User Workstation, page 17-8
- Collecting Diagnostics on the Cisco Unity Connection Server for IMAP Client Problems, page 17-8

Collecting Diagnostics from ViewMail for Outlook on the User Workstation

To troubleshoot problems with the Cisco ViewMail for Microsoft Outlook form, you can enable diagnostics on the user workstation.

To Enable Cisco ViewMail for Microsoft Outlook Diagnostics and View the Log Files on the User Workstation

Step 1 On the user workstation, on the Outlook Tools menu, select **Options**.

Step 2 Select the **ViewMail** tab.

Step 3 Check the **Turn on Diagnostic Traces** check box.

Step 4 Select **OK**.

Step 5 Reproduce the problem.

Step 6 Review the resulting log files by selecting **Help > Cisco ViewMail for Outlook > Email Log Files** and sending the resulting message with logs attached to an email address.

Collecting Diagnostics from ViewMail for Outlook 8.0 on the User Workstation

To troubleshoot problems with the Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 form, you can enable diagnostics on the user workstation.

To Enable ViewMail for Outlook Diagnostics and View the Log Files on the User Workstation

Step 1 On the user workstation, on the Outlook Tools menu, select **ViewMail for Outlook Options**.

Step 2 Select the **Diagnostics** tab.

Step 3 Enable the following diagnostics:

- Enable VMO Outlook Extension Diagnostics
- Enable VMO Multimedia Diagnostics

Step 4 If the problem is related to secure messages or recording and playback through the phone, enable the following diagnostics:

- Enable VMO Telephone Record/Playback Diagnostics
- Enable VMO HTTP Diagnostics

Step 5 Select **OK**.

Step 6 Reproduce the problem.

Step 7 Review the resulting log files, which are stored in the C:\Documents and Settings\All Users\Application Data\Cisco Systems\VMO\1.0\Logs folder.

Collecting Diagnostics on the Cisco Unity Connection Server for IMAP Client Problems

You can use Cisco Unity Connection traces to troubleshoot IMAP client problems from the server side.

Enable the following micro traces to troubleshoot IMAP client problems:

- SMTP (all levels)
- MTA (all levels)
- CuImapSvr (all levels)
- CsMalUmss (all levels)
- CML (all levels)

For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Login via IMAP fails for LDAPS if IP Address of LDAPserver is configured

It has been observed that login via IMAP clients for LDAP imported users, fails for LDAP-SSL case, if IP address of LDAP server is configured under LDAP authentication on CUCA page instead of FQDN or hostname of LDAP server. This would not impact the Java applications i.e. login via Cisco PCA would work fine for all the LDAP imported users. Customers who for some reason do not enable DNS must use the following workaround to use any non Java application to authenticate using SSL (CTI, TSP, etc.) The /etc/openldap/ldap.conf file contains information necessary for the openLDAP library to function properly. An issue involving certificates and openLDAP exists where openLDAP must be able to verify the certificate in order to connect to an LDAP server. The problem is, certificates are issued with a Fully Qualified Domain Name (FQDN), and if the customer's are not making use of DNS for any reason, they will be required to enter an IP Address on the LDAP Authentication web page (System->LDAP->LDAP Authentication). Part of the openLDAP verification is to match the FQDN with the server being accessed. Since the uploaded certificate uses FQDN and the web form is using IP Address, openLDAP will not be able to connect. The fix for this is for the customer to use DNS if possible.

CHAPTER 18

Troubleshooting Transcription (SpeechView) in Cisco Unity Connection 9.x

See the following sections for information on troubleshooting problems with the SpeechView feature:

Task List for Troubleshooting SpeechView

Do the following tasks in the order presented, as applicable.

Issues Related to Basic Configuration Settings

1. Check for warnings or errors in Cisco Unity Connection Administration:
   - On the System Settings > Licenses page. An error message on this page will alert you if you have a license violation. Confirm that your SpeechView usage is as you expect by looking at the number of SpeechView users listed under License Count. For more information about license issues, see the "Troubleshooting Licensing in Cisco Unity Connection 9.x" chapter.
   - On the Unified Messaging > SpeechView Transcription Service page.
   - On the System Settings > External Services > Transcription Service for SpeechView page.

   Many of the warning and error messages on these pages also include information on how to resolve the problem.

   Confirm that the Enabled check box is checked on the Unified Messaging > SpeechView Transcription Service page.

   Confirm that the Enabled check box is checked on the System Settings > External Services > Transcription Service for SpeechView page.

2. Confirm that the user belongs to a class of service for which the Use Standard SpeechView Transcription Service option is enabled.
   Similarly, confirm that the user belongs to a class of service for which the Use SpeechView Pro Transcription Service option is enabled.
3. Confirm that the user has a notification device configured with the Send Transcriptions of Voice Messages setting enabled.

Issues with a Proxy Server

4. If accessing the transcription service via a proxy server, troubleshoot the proxy server:
   a. In Cisco Unity Connection Serviceability, use the Voice Network Map tool to verify the health of the digital network. See the "Understanding the Voice Network Map Tool in Version 9.x" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.
   b. Verify that the server designated as a proxy system is configured to advertise transcription services.
   c. Continue with this task list on the proxy server.

Issues with the Transcription Service Configuration

5. If the transcription service registration is failing or times out, review the registration task execution results window for specific error messages.
6. If registration has succeeded, use the Test button to troubleshoot the transcription service configuration:
   a. In Cisco Unity Connection Administration, browse to the **Unified Messaging > SpeechView Transcription Service** page.

      In Cisco Unity Connection Administration, browse to the **System Settings > External Services > Transcription Service for SpeechView** page.
   b. Select the **Test** button.
   c. View the test task execution results for specific warnings and error messages.
7. If the test you ran above fails and the transcription service was previously working successfully but has suddenly stopped working, use the Reregister button to reestablish the registration with the external transcription service:
   a. In Cisco Unity Connection Administration, browse to the **Unified Messaging > SpeechView Transcription Service** page.

      In Cisco Unity Connection Administration, browse to the **System Settings > External Services > Transcription Service for SpeechView** page.
   b. Select the **Reregister** button.

      Another window displaying the results will open. The registration process normally takes several minutes.
   c. View the registration task execution results for specific warnings and error messages.
8. In Connection Serviceability, verify that the Connection SpeechView Processor and the Connection SMTP Server services are running. See the "Confirming That the Connection SpeechView Processor and Connection SMTP Server Services Are Running" section on page 18-4.

9. Run the SMTP test to verify that messages can successfully be sent from Connection to an external email account outside of your organization. This SMTP test will help you determine whether the registration problem is due to issues in the communication path to the third-party transcription service. See the "Running the SMTP Test to Verify the Outgoing and Incoming SMTP Path" section on page 18-4.
10. Generate the SpeechView Activity Summary Report to verify that the transcriptions are arriving at the Connection server. For more information, see the "Generating and Viewing Reports in Version 9.x" section in the "Using Reports in Version 9.x" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

Issues Related to User Expectations

11. Confirm that the message in question is of a type that is transcribed. The following messages are never transcribed:
    - Private messages
    - Broadcast messages
    - Dispatch messages

    Secure messages are transcribed only if the user belongs to a class of service for which the Allow Transcriptions of Secure Messages option is enabled.
12. Verify that the problem message was not already deleted by the user. When a transcription is received from the third-party transcription service, the transcription text is attached to the original voice message. If users delete a voice message before the transcription is received from the transcription service, the transcription text is attached to the deleted message. It is not considered a new message and will not be sent to a notification device.

Note If users belong to a class of service that is configured to move deleted messages to the Deleted Items folder, users can see the transcription in the Deleted Items folder of an IMAP client.

13. If the transcription service is unable to provide a transcription of a message, the user receives a message stating that the transcription cannot be provided and to call Connection to listen to the message. See the "Messages That Cannot Be Transcribed" section on page 18-6 for details.

Issues with Transcription Notifications

14. Troubleshoot the notification device configuration. See the "Troubleshooting Transcription Notifications" section on page 18-6.

Enabling Traces and Contacting Cisco TAC

15. If you still have problems after following all the troubleshooting steps described in this chapter, enable traces and contact the Cisco Technical Assistance Center (TAC). See the "Using Diagnostic Traces to Troubleshoot SpeechView" section on page 18-7.

Confirming That the Connection SpeechView Processor and Connection SMTP Server Services Are Running

The Connection SpeechView Processor service needs to be running only on the acting primary server of a Connection cluster server pair.

The Connection SMTP Server service needs to be running on both servers in a Connection cluster server pair.

Do the following procedure.

To Confirm That the Connection SpeechView Processor and Connection SMTP Server Services Are Running

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 On the Control Center – Feature Services page, under Optional Services, locate the **Connection SpeechView Processor** service.

Step 3 Confirm that the activate status for the Connection SpeechView Processor service is **Activated**. If the activate status is Deactivated, select **Activate**.

Step 4 Confirm that the service status for the Connection SpeechView Processor service is **Started**. If the service status is Stopped, select **Start**.

Step 5 Confirm that the activate status for the Connection SMTP Server service is **Activated**. If the activate status is Deactivated, select **Activate**.

Step 6 Confirm that the service status for the Connection SMTP Server service is **Started**. If the service status is Stopped, select **Start**.

Step 7 If using a Connection cluster, repeat Step 5 and Step 6 on the secondary server.

Running the SMTP Test to Verify the Outgoing and Incoming SMTP Path

The SMTP test is a CLI command that sends a test message to a specified email address. You then access the email account and reply to the test message without changing the subject line. The test passes when the response is received by the Cisco Unity Connection server. The success or failure of parts of the test help to narrow down whether the source of the problem is in the outgoing or incoming SMTP configuration.

To Run the SMTP Test to Verify the Outgoing and Incoming SMTP Path

Step 1 On the Cisco Unity Connection server, use the CLI (Command Line Interface) command **run cuc smtptest <email address>**. Use an email address that is outside of your organization.

For example, enter “run cuc smtptest johndoe@isp.com”.

Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 2 Sign in to the email account that you used in Step 1.

Step 3 If the outgoing message is not received at the email address that you specified in Step 1, do the following sub-steps to troubleshoot the problem:

a. Verify that the SMTP smart host setting is configured in Connection Administration. For details, see the "Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host" section in the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

b. Verify that Connection can reach the smart host by using the CLI command **utils network ping <smarthost>**.

c. Verify that the smart host is configured to route messages from the Connection server to the outside world.

d. Review the logs on the smart host server.

Step 4 Repeat Step 1 through Step 3 until the test message successfully arrives at the email address you specified in Step 1.

Step 5 Reply to the test message. Do not change the subject line.

Step 6 If the incoming reply message is not received by the CLI test, do the following sub-steps to troubleshoot the problem:

a. Verify that the email address entered in the Incoming SMTP Address field on the Unified Messaging > SpeechView Transcription Service page in Connection Administration is being routed correctly. It must be routed by your email infrastructure to the "stt-service" account on the Connection server domain.

Verify that the email address entered in the Incoming SMTP Address field on the System Settings > External Services > Transcription for SpeechView page in Connection Administration is being routed correctly. It must be routed by your email infrastructure to the "stt-service" account on the Connection server domain.

For example, if the Connection SMTP domain on the System Settings > SMTP Configuration > Server > SMTP Domain page in Connection Administration is "connection.example.com," and if the Incoming SMTP Address is "transcriptions@example.com," the email system must be configured to route transcriptions@example.com to stt-service@connection.example.com.

b. View the Connection SMTP Server component log files to see if the message reached Connection. The SMTP logs are located in diag_SMTP_*.uc. If you see "untrusted client connection refused" messages in the log files, you need to configure Connection to trust incoming traffic from your email system.

For details on configuring Connection to trust incoming traffic from your email system, see the "Configuring the Cisco Unity Connection Server to Accept Messages From Your Email System" section in the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

c. View the log files for your email infrastructure for additional clues.

Step 7 Repeat Step 5 through Step 6 until the test message reply is received.

Step 8 If the test continues to fail, enable traces and contact Cisco TAC. See the "Using Diagnostic Traces to Troubleshoot SpeechView" section on page 18-7.

Troubleshooting Transcription Notifications

Do the following procedure. Note that the problem with transcription notifications may be solved by any of the steps in the procedure, which are arranged in order of likelihood. After each step, retest transcription notifications, and if the problem has not been resolved, continue on to the next step in the procedure.

To Troubleshoot Transcription Notifications

Step 1 Confirm that messages are being transcribed by following Step 1. through Step 13. in the "Task List for Troubleshooting SpeechView" section on page 18-1.

Step 2 Confirm that the Send Transcriptions of Voice Messages setting is enabled for the SMS or SMTP notification device on the Edit Notification Device page for the user account in Cisco Unity Connection Administration.

Step 3 If the message is a secure message, confirm that the user belongs to a class of service that allows transcriptions of secure messages to be sent to notification devices.

Step 4 Test to see whether the SMS or SMTP notification device receives non-transcription messages by doing the following sub-steps:

a. Verify that the device is configured to notify the user for All Voice Messages.

b. Send a voice message to the user.

c. If the device is not receiving any notifications, see the "Troubleshooting Notification Devices in Cisco Unity Connection 9.x" chapter for further troubleshooting information.

Step 5 If these steps do not resolve the problem, enable traces and contact Cisco TAC. See the "Using Diagnostic Traces to Troubleshoot SpeechView" section on page 18-7.

Messages That Cannot Be Transcribed

The third-party transcription service may have problems transcribing messages if the recording is inaudible or if the sender was speaking in a language that is not supported by the transcription service. In these cases, the service will return a transcription that instructs the user to call Connection to listen to the message.

Using Diagnostic Traces to Troubleshoot SpeechView

You can use Cisco Unity Connection traces to troubleshoot problems with the SpeechView transcription feature.

Enable the following micro traces to troubleshoot SpeechView problems:

- MTA (level 10, 11, 12, 13)
- SMTP (all levels)
- SttClient (all levels)
- SttService (all levels)
- SysAgent (level 10, 11, 12, 16)
- Notifier (level 16, 21, 25, 30) —if you are troubleshooting problems with delivery to notification devices.

For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

CHAPTER 19

Troubleshooting Searching and Addressing in Cisco Unity Connection 9.x

See the following sections:

Troubleshooting Directory Handler Searches in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if callers report that they are unable to locate one or more users in a directory handler. See the following possible causes:

- The users are not configured to be listed in the directory. Verify the List in Directory setting on the Edit User Basics page for each user in Cisco Unity Connection Administration, or use Bulk Edit to configure the setting for multiple users at the same time.
- The search scope of the directory handler does not include the users. See the "Users Are Not Found in the Search Scope of the Directory Handler" section on page 19-1.
- For voice-enabled directory handlers, the voice-recognition engine does not recognize the names. See the "Voice Commands Are Recognized, But Names Are Not in Cisco Unity Connection 9.x" section on page 25-2.

Users Are Not Found in the Search Scope of the Directory Handler

If callers are unable to find specific users in a directory handler, check the search scope of the directory handler on the Edit Directory Handler Basics page in Cisco Unity Connection Administration. The search scope of a phone directory handler can be set to the entire server; to a specific class of service, system distribution list or search space; or to the search space of the call at the point that the caller reaches the directory handler. The search scope of a voice-enabled directory handler can be set to the entire server, to a specific search space, or to the search space of the call at the point that the caller reaches the directory handler.

If the search scope is set to the entire server, the user or users must be homed on the server on which the directory handler resides in order to be reachable from the directory handler.

If the search scope is set to a specific class of service, system distribution list, or search space, you can use Connection Administration to determine whether the target users belong to the class of service or distribution list or to a partition that is a member of the search space.

If the search scope is set to inherit the search space from the call, determine which search scope is in use when callers have difficulty reaching users in the directory handler. Note that depending on how the call comes in to the system and is routed, the search scope can differ from one call to another and can change during the course of the call. See the "Using Traces to Determine Which Search Space Is in Use During a Call in Cisco Unity Connection 9.x" section on page 19-3 for instructions on using traces to determine the inherited search scope.

Troubleshooting Message Addressing in Cisco Unity Connection 9.x

Message addressing involves the ability to select a desired recipient or recipients when creating a new message. Use the troubleshooting information in this section if users report that they are experiencing difficulties with message addressing. See the following:

Note For additional information about troubleshooting message addressing when it involves remote recipients at VPIM locations or at other digitally networked Cisco Unity Connection locations, see the "Troubleshooting Networking in Cisco Unity Connection 9.x" chapter.

Users Cannot Address to Desired Recipients

If a user is unable to find one or more desired recipients when attempting to address a message, start by verifying that the recipient user or contact account exists and that the name spelling or extension that the user is entering is correct.

If the user is attempting to blind address a message to a VPIM location by entering a number that is made up of the VPIM location DTMF Access ID and the mailbox number of the recipient, or by saying the digits of the mailbox number and the display name of the VPIM location (for example, "five five at Seattle office"), confirm that blind addressing is enabled for the VPIM location by checking the Allow Blind Addressing check box on the VPIM Location page in Cisco Unity Connection Administration.

If you have verified that the recipient account exists and matches the user search criteria or that blind addressing is enabled, and the user still cannot address to the desired recipient, the most likely cause is that the user search space does not include the partition of the target user, VPIM contact, or VPIM location. If the VPIM contact partition does not match the partition of the VPIM location to which the contact belongs, the search results depend on the method used to address the message as well as the partition and search space configuration. When users address messages to a VPIM mailbox by entering a VPIM location DTMF Access ID plus a remote user mailbox number, or when voice-recognition users say a name and location (for example, "John Smith in Seattle"), the action is allowed or denied based on the partition of the VPIM location. However, when users address to a VPIM contact by using

spell-by-name or by entering the local extension of the contact, or when voice-recognition users say the name of a contact without the location (for example, "John Smith"), the action is allowed or denied based on the partition of the VPIM contact, regardless of whether the partition of the VPIM location is out of scope for the user.

Users Cannot Address to a System Distribution List

When a user cannot address messages to a system distribution list, consider the following possible causes:

- The user must be given the correct class of service rights on the Class of Service > Edit Class of Service page in Cisco Unity Connection Administration. The class of service that the user is assigned to must have the Allow Users to Send Messages to System Distribution Lists check box checked.
- The user must know how to address to the list. If the user is using the phone keypad conversation, the user can enter the display name or extension of the list. If the user is using the voice-recognition conversation, the user can say the display name or one of the alternate names defined for the list in Connection Administration.
- As with other types of addressing, in order for a user to address messages to a system distribution list, the list must belong to a partition that is a member of the search space that is defined as the user search scope. Note that the distribution list members receive the message regardless of whether they are individually addressable in the search scope of the sending user.

Unexpected Results Are Returned When a User Addresses by Extension

If a user addresses a message by extension and hears an unexpected match, the most likely cause is the search space configuration. To make a match by extension, Cisco Unity Connection checks the search space of the user who is addressing the message. Connection searches the partitions in this search space in the order that they appear in the Assigned Partitions list in Cisco Unity Connection Administration, and returns the first result found. If your dial plan includes overlapping extensions, it is possible for the user to enter an extension that matches multiple users or other Connection objects and hear a match result that is different from what the user expects.

To resolve the issue, you may need to review the order of partitions in the search space that is assigned to the user, either in Connection Administration or by using the Dial Plan Report and Dial Search Scope Report in Cisco Unity Connection Serviceability. If the search space is set up correctly according to your dial plan, you can recommend that the user address messages by spelling or saying the name of the recipient; in this case, if there are multiple matches on the name, Connection returns each match.

Using Traces to Determine Which Search Space Is in Use During a Call in Cisco Unity Connection 9.x

The search scope of a call is initially set to a particular search space by the call routing rule that first processes the call, although the scope may change during the course of the call.

To determine which search space is being used at each point in a call, enable the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

CHAPTER 20

Troubleshooting Networking in Cisco Unity Connection 9.x

Revised June 3, 2013

See the following sections:

Troubleshooting Intersite Networking Setup in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if you have difficulty creating an intersite link between two site gateways (regardless of whether you are linking two Cisco Unity Connection sites or a Connection site and a Cisco Unity site). See the following sections:

"Unable to Contact the Remote Site" Error When Manually Creating an Intersite Link on the Cisco Unity Connection 9.x Site Gateway

When you create an intersite link in Cisco Unity Connection Administration by using the Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files option, the site gateway on which you are creating the link reads the fully-qualified domain name (FQDN) for the remote site gateway from the configuration file that you upload, and attempts to resolve the FQDN by using DNS. If DNS has not been configured on the Cisco Unity Connection site gateway, or the remote site gateway that you are linking to cannot be resolved via DNS, Connection Administration

displays the error, “Unable to contact the remote site. You may choose to go ahead and create a link to this site, but synchronization with this site will not begin until communication can be established without errors. Do you wish to continue?” (The use of DNS name resolution is optional with Connection.)

When you see this error, do the following procedure to continue creating the link and to enable the synchronization tasks, which are automatically disabled when Connection encounters this error condition.

To Manually Create an Intersite Link When the Remote Site Gateway Cannot Be Resolved Via DNS

Step 1 On the New Intersite Link page, with the error displayed in the Status message, select **Link**. (If you have navigated away from the page, expand **Networking**, expand **Links**, and select **Intersite Links**. Then select **Add**. Select **Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files**, and select **Browse** to upload the Remote Site Configuration File. Configure other settings on the page as applicable, and select **Link**. Select **Link** again when the error is displayed in the Status message.)

Step 2 On the Edit Intersite Link page, change the **Hostname** value from the FQDN to the IP address of the remote site gateway.

Step 3 Select **Save**.

Step 4 Enable the directory synchronization task by doing the following sub-steps:

a. In the Related Links field in the upper right corner of the Edit Intersite Link page, select **Remote Site Directory Synchronization Task**, and then select **Go**.

Tip Alternatively, you can navigate to the task by expanding **Tools**, selecting **Task Management**, and selecting the **Synchronize Directory With Remote Networ**k task on the Task Definitions page. To edit the task schedule, on the Task Definition Basics page, select **Edit**, and then select **Task Schedules**.

b. Check the **Enabled** check box.

c. Configure the task to run on the desired schedule. (By default, the task runs every 15 minutes.)

d. Select **Save**.

Step 5 To return to the list of tasks, select **Task Definition**, and then select **Task Definitions**.

Step 6 Optionally, enable the voice name synchronization task by doing the following sub-steps:

a. On the Task Definitions page, select **Synchronize Voice Names with Remote Network**.

b. On the Task Definition Basics page, select **Edit**, and then select **Task Schedules**.

c. Check the **Enabled** check box.

d. Configure the task to run on the desired schedule. (By default, the task runs every 15 minutes.)

e. Select **Save**.

"Hostname Entered Does Not Match That on The Remote Site Certificate" Error When Manually Creating an Intersite Link on the Cisco Unity Connection 9.x Site Gateway

When you create an intersite link in Cisco Unity Connection Administration by using the Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files option, the site gateway on which you are creating the link reads the fully-qualified domain name (FQDN) for the remote site gateway from the configuration file that you upload, and, if you check the Use Secure Sockets Layer (SSL) check box, verifies whether the FQDN matches the servername on the remote site gateway web SSL certificate (the certificate for browsing to the machine over HTTPS). If the values do not match, Connection Administration displays the error, "Hostname entered does not match that on the remote site certificate."

When you see this error, you can do the following procedure to repeat the link creation process and to circumvent the error by checking the Ignore Certificate Errors check box.

To Manually Create an Intersite Link When the Remote Site Gateway Hostname Does Not Match the Name on the Certificate

Step 1 On the New Intersite Link page, select **Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files**, and select **Browse** to upload the Remote Site Configuration File.

Step 2 For Transfer Protocol, check the **Ignore Certificate Error**s check box.

Step 3 Configure other settings on the page as applicable, and select **Link**.

"Unable to Link to the Specified Remote Site. Cause: Failed to Assess the Current Network Size" Error When Creating an Intersite Link on the Cisco Unity Connection 9.x Site Gateway

When you create an intersite link in Cisco Unity Connection Administration, the Connection site gateway checks to see if the combined number of users and contacts on the gateway after the link is created would exceed the user and contact limit. It also checks if the combined number of system distribution lists on the gateway would exceed the system distribution list limit.

If the site gateway is unsuccessful at performing these checks, Connection Administration displays the error, "Unable to Link to the Specified Remote Site. Cause: Failed to Assess the Current Network Size." If you see this error, you can view the default traces for the Connection Tomcat Application service (trace log filenames matching the pattern diag_Tomcat_*.uc) and search the file for the term "GetDirectoryCurrentSize." For detailed instructions on viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

For more information on the directory size limits, see the "Cisco Unity Connection 9.x Directory Size Limits" section in the "Overview of Networking Concepts in Cisco Unity Connection 9.x" chapter of the *Networking Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.

"Failed to Link to This Remote Site As This Specified Location Is Already Part of the Network" Error When Creating an Intersite Link on the Cisco Unity Connection 9.x Site Gateway

The error "Failed to link to this remote site as this specified location is already part of the network" is displayed when you attempt to create an intersite link in Cisco Unity Connection Administration under any of the following conditions:

- You attempt to create an intersite link from a location to the location itself.
- You attempt to create an intersite link from one location to another location that is a member of the same Connection site.
- You attempt to create an intersite link from a location on one site to a location on another site, and the sites are already linked.

If you see this error, check the hostname information or the configuration file that you are using to create the link. Verify that you are linking to the correct remote site gateway and that a link does not already exist between sites, then retry the linking process.

Troubleshooting Message Addressing in Cisco Unity Connection 9.x

Message addressing involves the ability to select recipients when creating a new message.

Use the troubleshooting information in this section if users report that they are unable to address messages to recipients on another voice messaging system. See the following sections:

- Cisco Unity Connection Users Cannot Address Messages to Remote Users, Contacts, or System Distribution Lists, page 20-4
- Cisco Unity Connection Users Cannot Address Messages to Recipients at a VPIM Location, page 20-8
- Cisco Unity Connection Users Cannot Blind Address Messages to a Mailbox at a VPIM Location, page 20-8

If a message is successfully created and sent to a remote recipient but is not received by the recipient, see the "Troubleshooting Message Transport in Cisco Unity Connection 9.x" section on page 20-9. For addressing issues involving only local recipients on the same Cisco Unity Connection server, see the "Troubleshooting Searching and Addressing in Cisco Unity Connection 9.x" chapter.

Cisco Unity Connection Users Cannot Address Messages to Remote Users, Contacts, or System Distribution Lists

If Cisco Unity Connection users are unable to address messages to remote objects within a Cisco Unity Connection site or on a linked Connection or Cisco Unity site, do the following tasks in the order presented:

1. Check for the presence of the remote object in Cisco Unity Connection Administration on the location on which users are experiencing the problem. This indicates whether the remote object has been replicated. If the object is not found, see the "Troubleshooting Directory Synchronization in Cisco Unity Connection 9.x" section on page 20-11 for further troubleshooting steps.

2. Check the partition and search space configuration. The remote object to which the message is being addressed must belong to a partition that is a member of the search space configured as the search scope for the user. See the "Checking the Partition and Search Space Configuration for Addressing to Remote Objects" section on page 20-5.
3. Turn on the CDE micro trace (level 12 CDL Access). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Checking the Partition and Search Space Configuration for Addressing to Remote Objects

If you have only a single Cisco Unity Connection site, when you initially set up the site between locations, users who are homed on one location are not able to address messages to users at other locations, because the users on each location are in separate partitions and use search spaces that do not contain the partitions of users on the other locations. After initial replication completes between the locations, you can reconfigure your search spaces to include partitions that are homed on other servers, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a remote location. (Note that while both partitions and search spaces are replicated between locations, you cannot assign users or other objects to a partition that is homed on another location.)

If you have linked one Cisco Unity Connection site to another Connection site, partitions and search spaces are replicated between the sites. However, when you initially set up the link between sites, the users are in separate partitions and use search spaces that do not contain the partitions of users on the locations in the other site. After initial replication completes between the sites, you can reconfigure your search spaces to include partitions that are homed on the remote site, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a location in the remote site.

When you link a Cisco Unity Connection site and a Cisco Unity site, a partition is automatically created in the Connection directory for each Cisco Unity server, and all Cisco Unity users and replicated system distribution lists that are homed on the server are placed in the partition. However, the partition is not automatically added to search spaces on the Connection locations. In order for Connection users to have permission to address messages to Cisco Unity users or replicated distribution lists, you must add the partition to the search spaces used by those Connection users. Note that the order a partition appears in a search space is important if users address messages by extension. If, for example, Connection and Cisco Unity users have overlapping 4-digit extensions and you want Connection users to be able to reach other Connection users by their 4-digit primary extension and reach Cisco Unity users by a unique 7-digit alternate extension, make sure that the Cisco Unity partition appears after any Connection partitions that contain the overlapping 4-digit extensions.

At a minimum, when a Connection user is unable to address to a remote user or other object, you can do the following procedure to check whether the partition of the remote object is in the search space of the user that is attempting to address to the object.

To Check Whether the Partition of a Remote Object Belongs to the Search Space of a Cisco Unity Connection User

Step 1 In Cisco Unity Connection Administration on the location on which the Cisco Unity Connection user who is having the addressing problem is homed, browse to the Edit page for the object the user is trying to address to:

- For a remote user, select **Users**. On the Search Users page, use the Search Limits fields and the search criteria to find the remote user. Select the user alias of the remote user to display the Edit User Basics page.

- For a remote contact, select **Contacts**. On the Search Contacts page, use the Search Limits fields and the search criteria to find the remote contact. Select the alias of the remote contact to display the Edit Contact Basics page. (Note that contacts are only replicated within a single site.)
- For a remote system distribution list, expand **Distribution Lists**, then select **System Distribution Lists**. On the Search Distribution Lists page, use the Search Limits fields and the search criteria to find the remote system distribution list. Select the alias of the remote list to display the Edit Distribution List Basics page. (Note that, depending on the intersite link and distribution list configuration, distribution lists may not be replicated across an intersite link.)

Step 2 On the Edit page for the object, note the value in the Partition field.

Step 3 Note the search space of the Cisco Unity Connection user who is having the addressing problem:

a. Select **Users**.

b. On the Search Users page, use the Search Limits fields and the search criteria to find the user who is having the addressing problem.

c. Select the alias of the user to display the Edit User Basics page.

d. On the Edit User Basics page, note the value of the Search Scope field.

Step 4 Check the configuration of the search space that you noted in Step 3:

a. Expand **Dial Plan**, and select **Search Spaces**.

b. On the Search Search Spaces page, use the Search Limits fields and the search criteria to find the search space that you noted in Step 3.

c. Select the name of the search space.

d. On the Edit Search Space page, if the partition that you noted in Step 2 is not in the Assigned Partitions list, find it in the Unassigned Partitions list, select it, and click the up arrow to move it to the Assigned Partitions list. Then click **Save**.

Note If the search space is homed on another location, select the link in the Status message at the top of the page to edit the search space from the remote location. A new window opens to Connection Administration on the remote location.

Cisco Unity Users Cannot Address Messages to Cisco Unity Connection Users or System Distribution Lists

If Cisco Unity users are unable to address messages to users on a Connection site to which Cisco Unity is linked via an intersite link (also known as Connection Networking), do the following tasks in the order presented:

1. Check for the presence of the Connection user object as a Connection Networking subscriber in the Cisco Unity Administrator. This indicates whether the Connection user object has been replicated. If the object is not found, see the "Troubleshooting Directory Synchronization in Cisco Unity Connection 9.x" section on page 20-11 for further troubleshooting steps.
2. If the problem involves addressing by extension, check to see if the Connection user object has an extension in Cisco Unity, and if so, check whether the extension matches the format that Cisco Unity users are expecting. See the "Troubleshooting Cisco Unity Connection User Extension Creation in Cisco Unity" section on page 20-7.

Troubleshooting Cisco Unity Connection User Extension Creation in Cisco Unity

When you link a Cisco Unity Connection site and aCisco Unity site, the Connection user and system distribution list objects that are created in the Cisco Unity directory belong to the dialing domain that is configured on the Cisco Unity site gateway. Because the Connection search space and partition design accommodates overlapping extensions and may include users who have a primary extension and alternate extensions in different partitions, you must choose how to map Connection extensions to the Cisco Unity Dialing Domain. To do so, for each Connection location, you specify a single partition that Cisco Unity pulls extensions from. (In Cisco Unity Connection Administration, you configure the Local Partition That Cisco Unity Users Can Address to By Extension field on the Edit Location page for the local location.)

When users from a particular Connection location are replicated to Cisco Unity, only extensions belonging to Local Partition That Cisco Unity Users Can Address to By Extension are replicated to Cisco Unity. Because extensions within a dialing domain must be unique, the collection of all partitions chosen across the Connection site should not contain duplicates of any extension. When the collection includes duplicate extensions, or extensions that already exist in the Cisco Unity site gateway Dialing Domain, one or more extensions are omitted from the Cisco Unity directory. When this occurs, warnings appear in the Cisco Unity application event log indicating the owner of each omitted extension. After remedying any conflicts, you may need to do a manual resynchronization on the Cisco Unity site gateway (by selecting Total Sync on the Network > Connection Networking Profile page in Cisco Unity Administrator) in order to update the extensions.

It is also possible for a Connection user to not have any extensions belonging to the Local Partition That Cisco Unity Users Can Address To By Extension configured on the server on which the user is homed. In this case, as in other cases where the Connection user object is created without an extension, Cisco Unity users will not be able to address to the user by extension.

If the problem involves many user extensions on the same Connection location, you may need to change the partition chosen as the Local Partition That Cisco Unity Users Can Address to By Extension for the location. Do the following procedure to check or change this value.

To Configure the Partition that Cisco Unity Users Can Address To for a Cisco Unity Connection Location

Step 1 In Cisco Unity Connection Administration on the Connection location, expand **Networking**, then select **Locations**.

Step 2 Expand **Local Site** and select the display name of the local location (the location on which you are accessing Connection Administration).

Step 3 Under Local Partition That Cisco Unity Users Can Address To By Extension, for Partition, select the name of the partition to use.

Step 4 Select **Save**.

Cisco Unity Connection Users Cannot Address Messages to Recipients at a VPIM Location

Addressing to a particular recipient at a VPIM location can fail for one of the following reasons:

- Blind addressing is disabled for the VPIM location, and no VPIM contact exists for the recipient. If you are relying on automatic VPIM contact creation to populate VPIM contacts based on incoming messages, it is possible that contact creation is not set up properly for this location, or that no messages have been received from the remote user. Check the settings on the Contact Creation page for the VPIM location in Cisco Unity Connection Administration.
- A VPIM contact exists, but users are unable to locate it because the extension is incorrect or the contact name does not match user searches. Check the VPIM contact configuration in Connection Administration.
- Users are attempting to blind address to VPIM recipients, but the DTMF Access ID of the VPIM location is incorrect or does not match the pattern users are attempting to enter when addressing. Check the value of the DTMF Access ID setting on the Edit VPIM Location page in Connection Administration, and confirm that users are aware of the correct value.
- The user search scope does not include the partition of the VPIM contact or VPIM location. If the VPIM contact partition does not match the partition of the VPIM location to which the contact belongs, the search results depend on the method used to address the message as well as the partition and search space configuration. When users address messages to a VPIM mailbox by entering a VPIM location DTMF Access ID plus a remote user mailbox number, or when voice-recognition users say a name and location (for example, “John Smith in Seattle”), the action is allowed or denied based on the partition of the VPIM location. However, when users address to a VPIM contact by using spell-by-name or by entering the local extension of the contact, or when voice-recognition users say the name of a contact without the location (for example, “John Smith”), the action is allowed or denied based on the partition of the VPIM contact, regardless of whether the partition of the VPIM location is out of scope for the user. In Connection Administration, on the Edit User Basics page for the user, check which search space is configured as the search scope. Then check which partition is configured for the VPIM contact (on the Edit Contact Basics page) or for the VPIM location (on the Edit VPIM Location page), as applicable. Finally, check the Edit Search Space page for the user search space to determine whether the partition appears in the Assigned Partitions list.

Cisco Unity Connection Users Cannot Blind Address Messages to a Mailbox at a VPIM Location

Blind addressing allows users to send messages to recipients at the VPIM location even if the recipients are not defined as contacts in the Cisco Unity Connection directory. If blind addressing is not working, confirm that you have enabled it for an individual VPIM location by checking the Allow Blind Addressing check box on the VPIM Location page in Cisco Unity Connection Administration. When this check box is checked for a location, users can address messages to recipients at this location by entering a number that is made up of the VPIM location DTMF Access ID and the mailbox number of the recipient, or by saying the digits of the mailbox number and the display name of the VPIM location (for example, “five five at Seattle office”).

Troubleshooting Message Transport in Cisco Unity Connection 9.x

Cisco Unity Connection uses SMTP to exchange voice messages with other systems. This includes VPIM messages, messages between users within a Connection site, messages to users on a different Connection site or on a Cisco Unity site, and messages sent to Connection by IMAP clients or forwarded by Connection to the relay address configured on the Message Actions page for a user.

In order for a Connection system to exchange SMTP messages with other voice messaging systems or Connection locations, the system must either be able to directly access TCP/IP port 25 on the remote system, or be configured to deliver messages to an SMTP smart host that can relay messages to the system. When VPIM Networking is in use within a Connection networking site, typically you create each VPIM location on only one Connection server in the site; the other locations in the site then forward messages that are addressed to users at the VPIM location to the Connection server that homes the VPIM location for delivery. In this case, only this Connection server needs SMTP connectivity (either directly or through a smart host) with the remote messaging system.

When a message is recorded by a Connection user for delivery to a remote system, the message is first processed by the Message Transfer Agent (MTA). This service formats the message. For example, for a VPIM message, the MTA formats the To: and From: fields on the message, sets the content-type of the message to multipart/Voice-Message, and sets other header properties. It then places the message in a pickup folder on the Connection server. The SMTP service periodically checks the pickup folder for messages, removes a message from the folder, determines the destination server from the message header, establishes an SMTP connection to the correct server, and sends the message. The process is reversed when Connection receives an incoming message via SMTP—the message is first processed by the SMTP service, then the MTA service.

Use the troubleshooting information in this section if you are experiencing difficulties with message transport. See the following sections:

- Messages Sent from Users on One Cisco Unity Connection 9.x Location Are Not Received by Users on Another Cisco Unity Connection Location, page 20-9
- Replies to Messages Sent by Remote Senders are Not Delivered, page 20-10
- Messages Sent from a VPIM Location Are Not Received by Cisco Unity Connection Users, page 20-10
- Messages Sent from Cisco Unity Connection Are Not Received by Users at a VPIM Location, page 20-11

Messages Sent from Users on One Cisco Unity Connection 9.x Location Are Not Received by Users on Another Cisco Unity Connection Location

In general, messages that are successfully addressed to a remote user by using the phone interface should be delivered as long as SMTP connectivity is established between the locations. A notable exception occurs when a user replies to all recipients of a received message, and some of those recipients are not in the search scope of the replying user. In this case, the replying user receives a non-delivery receipt for any recipient who is not in the search scope.

Messages sent by using an IMAP client to a remote user can fail if the profile information for the remote user (specifically, the SMTP proxy address information of the remote user) has not fully replicated to the Connection location of the sending user. To diagnose and correct this condition, see the "Troubleshooting Directory Synchronization in Cisco Unity Connection 9.x" section on page 20-11.

If the issue does not appear to be related to the partition and search space configuration or directory replication, you may be able to further diagnose the problem by turning on the Message Tracking Traces macro trace. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Replies to Messages Sent by Remote Senders are Not Delivered

In cases where you have recently added a location to a site or linked sites, it is possible for messages to be received from remote senders whose user object has not yet replicated to a location. If a user attempts to reply to a message that was sent by a sender whose user object has not yet replicated, the reply is not delivered, and the sender receives a non-delivery receipt (NDR). When this happens, the user who attempted the reply can resend the reply after the user object of the original message sender has replicated, and the reply will be successfully delivered.

Messages Sent from a VPIM Location Are Not Received by Cisco Unity Connection Users

In order for incoming VPIM messages to be received and processed correctly, the following are required:

- SMTP connectivity must be available between the originating voice messaging system and Cisco Unity Connection.
- If messages from the originating voice messaging server are routed through a smart host that is different from the one that is configured on the System Settings > SMTP Configuration > Smart Host page in Cisco Unity Connection Administration, the IP address of this smart host must be added to the IP Address Access List as an allowed connection. (On the System Settings > SMTP Configuration > Server page, select Edit > Search IP Address Access List to view or modify the access list.)
- The domain name in the incoming message "From" field must match the Remote VPIM Domain Name value that is defined for the VPIM location in Connection Administration.
- If a Remote Phone Prefix value is defined for the VPIM location, the mailbox number in the incoming message "From" field must begin with the prefix digits.
- If a Cisco Connection Phone Prefix is defined for the VPIM location, the mailbox number in the incoming message "To" field must begin with the prefix digits.
- The Connection users receiving the message must be in a partition that is a member of the search space that is defined as the search scope of the VPIM location on the receiving server.
- If intersite networking is in use, the VPIM location must be configured on a Connection location within the Connection site on which the recipient is homed. VPIM locations and contacts are replicated within a site but are not replicated across intersite links, and site gateways do not relay VPIM messages to other sites.

You can verify SMTP connectivity and check the format of the "From" and "To" fields by turning on all levels of SMTP micro traces. ("MAIL FROM" and "RCPT TO" appear in the SMTP trace logs.) In addition, when you turn on all levels of MTA micro traces, the MTA log contains information about the processing of the message, including messages describing prefix processing errors. You can use the message ID listed at the end of the output file path name in the SMTP logs (for example, csUnitySmtp-30-1223425087697), to locate a message in the MTA log, or search by the recipient address (for example, 5551212@receiving-server-domain.com). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Messages Sent from Cisco Unity Connection Are Not Received by Users at a VPIM Location

In order for outgoing VPIM messages to be received and processed correctly, the following are required:

- SMTP connectivity must be available between Cisco Unity Connection and the receiving voice messaging system, either through direct TCP/IP connectivity to port 25, or through an SMTP smart host. (You can configure the SMTP smart host on the System Settings > SMTP Configuration > Smart Host page in Cisco Unity Connection Administration.)
- The audio attachment on the VPIM message must be in a format that is playable on the remote system. If the remote voice messaging system is not Connection or Cisco Unity, you may need to configure the Outbound Messages setting for the VPIM location in Cisco Unity Connection Administration to use the G.726 codec to transcode the audio format.

As with incoming VPIM messages, when troubleshooting outgoing messages, we recommend that you start by turning on all MTA and SMTP micro traces. When examining the logs for outgoing message issues, start with the MTA log first, then review the SMTP log. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Troubleshooting Directory Synchronization in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if you are experiencing difficulties with directory synchronization either within a Cisco Unity Connection site (intrasite networking) or between sites (intersite networking). See the following sections:

Troubleshooting Directory Synchronization within a Cisco Unity Connection Site in Cisco Unity Connection 9.x

Within a site, each location uses SMTP to exchange directory synchronization information and messages directly with every other location. Use the troubleshooting information in this section if you are experiencing difficulties with directory synchronization within a single Connection site. See the following sections:

Unique Sequence Numbers (USNs) Are Mismatched Between Locations

The Connection Locations pages in Cisco Unity Connection Administration provide information about the status of replication between locations. On the Edit Connection Location page for a remote location, the Last USN Sent, Last USN Received, and Last USN Acknowledged fields indicate the sequence numbers of replication messages sent to and from the remote location. When two locations are fully synchronized, the Last USN Sent and Last USN Acknowledged values on the location that is sending replication updates should equal the Last USN Received on the location that is receiving updates.

During replication, it is normal for the Last USN Acknowledged value to lag behind the Last USN Sent value.

During a push synchronization, the Last USN Sent may display a very large value while the Last USN Acknowledged shows a much smaller value. This is normal. Monitor the Last USN Acknowledged to make sure it continues increasing toward the Last USN Sent value. If it does not, see the "Manual Directory Replication Is Stalled" section on page 20-13.

You can also use the Voice Network Map tool in Cisco Unity Connection Serviceability to check replication status within a site. The tool is particularly useful because it allows you to view replication status for all locations in the network from one place, so that you can quickly locate replication problems within a site. For more details, select Help > This Page from within the tool, or see the "Understanding the Voice Network Map Tool in Version 9.x" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

Automatic Directory Replication Is Stalled

Revised April 23, 2013

Directory changes on one Cisco Unity Connection server are automatically propagated to other locations in the site. If either the Last USN Acknowledged value that is displayed on the sending location or the Last USN Received value that is displayed on the receiving location stops incrementing toward the Last USN Sent value that is displayed on the sending location, replication may be stalled. This can happen when a Connection location receives an update to an object that depends on another object about which it has not received information. For example, the addition of a member to a distribution list depends on the presence of a user record for the member being added. If the location has not received the information about the user record, it waits for a default of five minutes to see if the directory message containing the user record information arrives to satisfy the dependency.

The reasons of stalled replication can be as follows:

- SMTP not working on either of the node or all nodes.
- Connection Digital Networking Replication Agent service not activated on either of the node or all nodes.
- Duplicate data may exist.

In most cases, the problem should resolve itself after the five minute time-out, at which point the receiving Connection system requests that the record be re-sent. If the problem is not resolved, use the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to check the Application System log to see if any errors have been reported by the CuReplicator application. For information on using RTMT to view system logs, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

You may also want to turn on Digital Networking macro traces to diagnose a replication issue. For detailed instructions on enabling intrasite networking replication traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Manual Directory Replication Is Stalled

When an administrator initiates a manual push or pull of the directory between two Cisco Unity Connection locations, the Push Directory or Pull Directory status displayed on the Networking > Connection Locations page for the remote location in Cisco Unity Connection Administration may indicate that replication is in progress, but the Last USN Acknowledged or Last USN Received values on the Edit Connection Location page may not be changing. If this problem occurs, try stopping the push or pull operation by checking the check box next to the display name of the remote location on the Connection Locations page and selecting Stop Push (if the Push Directory status for that location indicates a push is in progress) or Stop Pull (if the Pull Directory status for that location indicates a pull is in progress). You can then restart the manual replication.

Push and Pull Status Are Mismatched Between Locations

When an administrator initiates a manual push or pull of the directory between two Cisco Unity Connection locations, the Push Directory status displayed on the Networking > Links > Intrasite Links page in Cisco Unity Connection Administration on the sending location should match the Pull Directory status displayed in Connection Administration on the receiving location (for example, both should display In Progress during replication).

If the status does not match, wait at least five minutes. If it still does not match, you may be able to correct the mismatch by doing the following procedure.

To Resynchronize Push and Pull Status Between Locations

Step 1 In Cisco Unity Connection Administration on the location that displays Idle status for the push or pull, check the check box next to the display name of the mismatched location, and select **Push Directory To** or **Pull Directory From** to start the operation that should display In Progress.

For example, if location one shows a push is in progress and location two shows a pull is idle, on location two, check the check box next to the location one display name and select Pull Directory From.

Step 2 When the operation status displays as In Progress, wait a minute, then recheck the check box for the remote location and stop the operation by selecting either **Stop Push** or **Stop Pull**, as applicable.

Troubleshooting Directory Synchronization Between Two Cisco Unity Connection Sites

Replication between sites is accomplished by means of a Feeder service and a Reader service (also referred to as the FeedReader) running on each site gateway. The Reader service periodically polls the remote site gateway for any directory changes since the last poll interval. The Feeder service checks the change tracking database for directory changes and responds to poll requests with the necessary information. The Feeder service is implemented as a web site that returns directory information in XML format when it receives a request from the remote Reader. Because directory information includes names and extensions, it is treated as confidential, and authentication is required to access the feed. We also recommend that you configure SSL on each site gateway in order to encrypt the directory information.

The synchronization that occurs after two sites are first joined can take anywhere from a few minutes to a few hours depending on the directory size. Later updates will only synchronize changes since the last cycle, unless you manually request a full resynchronization.

On a Connection site gateway, you can configure the schedule on which the Reader polls the remote Feeder for directory data, and the schedule on which it polls for recorded names. You can access the schedules in Cisco Unity Connection Administration on the Tools > Task Management page by selecting either the Synchronize Directory With Remote Network task or the Synchronize Voice Names With Remote Network task.

Table 20-1 lists some of the tools you can use to collect information about the operation of the Feeder and Reader applications for intersite networking.

Table 20-1 Troubleshooting Tools for Intersite Replication Between Cisco Unity Connection Sites

Application	Troubleshooting Tool(s)
Reader	• The Networking > Links > Intersite Links > Edit Intersite Link page displays statistics about the number of replicated objects and object changes, the time of last synchronization, and the last time an error occurred during synchronization. • Enable FeedReader micro trace levels 00, 01, 02, 03, 10, and 14. See the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter for instructions.
Feeder	• Enable Feeder micro trace levels 00, 01, 02, and 03. See the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter for instructions.

If you want to manually start an incremental update of the directory on either site, you can do so by using the Sync button on the Networking > Links > Intersite Links page in Cisco Unity Connection Administration on the Connection site gateway. To initiate a full resynchronization of the entire directory, use the Resync All button on the same page.

Troubleshooting Directory Synchronization Between a Cisco Unity Connection Site and a Cisco Unity Site

Replication between sites is accomplished by means of a Feeder service and a Reader service running on each site gateway. The Reader service periodically polls the remote site gateway for any directory changes since the last poll interval. The Feeder service checks the change tracking database for directory changes and responds to poll requests with the necessary information. The Feeder service is implemented as a web site that returns directory information in XML format when it receives a request from the remote Reader. Because directory information includes names and extensions, it is treated as confidential, and authentication is required to access the feed. We also recommend that you configure SSL on each site gateway in order to encrypt the directory information.

The synchronization that occurs after two sites are first joined can take anywhere from a few minutes to a few hours depending on the directory size. Later updates will only synchronize changes since the last cycle, unless you manually request a full resynchronization.

On the Connection site gateway, you can configure the schedule on which the Reader (also referred to as the FeedReader in Connection) polls the remote Feeder for directory data, and the schedule on which it polls for recorded names. In Cisco Unity Connection Administration on the site gateway, you can access the schedules on the Tools > Task Management page by selecting either the Synchronize Directory With Remote Network task or the Synchronize Voice Names With Remote Network task.

On the Cisco Unity site gateway, you can enable or disable synchronization of recorded names, and configure the interval at which the Reader polls the Connection Feeder for directory updates and recorded names. In the Cisco Unity Administrator on the site gateway, you can access both settings (Synchronize Voice Names and Feeder Interval) on the Networking > Connection Networking page.

Note that unlike the Connection Reader, which has separate configurable schedules for polling directory data and recorded names, the Cisco Unity Reader polls for both (if recorded name synchronization is enabled) during each cycle.

Table 20-2 lists the tools and details you can use to collect information about the operation of the Feeder and Reader applications for both Cisco Unity Connection and Cisco Unity.

Table 20-2 Troubleshooting Tools for Intersite Replication Between Cisco Unity Connection and Cisco Unity

Application	Troubleshooting Tool(s)
Cisco Unity Connection Reader	• The Networking > Links > Intersite Links > Edit Intersite Link page displays statistics about the number of replicated objects and object changes, the time of last synchronization, and the last time an error occurred during synchronization. • Enable FeedReader micro trace levels 00, 01, 02, 03, 10, and 14. See the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter for instructions.
Cisco Unity Connection Feeder	• Enable Feeder micro trace levels 00, 01, 02, and 03. See the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter for instructions.
Cisco Unity Reader	• The Networking > Connection Networking page in the Cisco Unity Administrator on the site gateway displays statistics about the number of replicated objects and object changes, the time of last synchronization, and the last time an error occurred during synchronization. • The Cisco Unity Reader logs operational and error messages to the Windows Application Event Log. • For additional troubleshooting information, use the Cisco Unity Diagnostic Tool to configure the CuDirReader micro traces (all levels except level 2). Note that there are several threads involved in reading objects from Connection and writing them to SQL and to Active Directory. To follow an object through the log file, search by its Unique Sequence Number (USN), the ID of the object, or the alias. For instructions, see the "Diagnostic Trace Utilities and Logs in Cisco Unity 9.x" chapter of the *Troubleshooting Guide for Cisco Unity Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/9x/troubleshooting/guide/9xcutsgx.html. **Caution** The log file may grow very large if you have Reader traces turned on while the initial synchronization or a full resynchronization is in progress between sites.

Table 20-2 Troubleshooting Tools for Intersite Replication Between Cisco Unity Connection and Cisco Unity (continued)

Application	Troubleshooting Tool(s)
Cisco Unity Feeder	• Use the Cisco Unity Diagnostic Tool to configure the CuFeeder micro traces. The trace logs can be found in diag_w3wp. For instructions, see the "Diagnostic Trace Utilities and Logs in Cisco Unity 9.x" chapter of the *Troubleshooting Guide for Cisco Unity Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/9x/troubleshooting/guide/9xcutsgx.html.

If you want to manually start an incremental update of the directory on either site, you can do so by using the Sync button on the Networking > Links > Intersite Links page in Cisco Unity Connection Administration on the Connection site gateway or by using the Sync Now button on the Network > Connection Networking page in the Cisco Unity Administrator on the Cisco Unity site gateway. To initiate a full resynchronization of the entire directory, use the Resync All button on the Networking > Links > Intersite Links page in Cisco Unity Connection Administration on the Connection site gateway or the Total Sync button on the Network > Connection Networking page in the Cisco Unity Administrator on the Cisco Unity site gateway.

Cross-Server Sign-In and Transfers in Cisco Unity Connection 9.x

When a Cisco Unity Connection servers is networked with other Connection or Cisco Unity locations, cross-server features can be configured such that:

- Calls are transferred to users who are not associated with the local server, according to the call transfer and screening settings of the user who is receiving the transfer. (This includes calls that are transferred from the automated attendant or the corporate directory, and live reply calls that are transferred when a user listens to a message and chooses to reply by calling the sender.) This functionality is referred to as a cross-server transfer.
- When calling from outside the organization to sign in, users—no matter which is their home server—can call the same number and are transferred to the applicable home server to sign in. This functionality is referred to as a cross-server sign-in.

Use the troubleshooting information in this section if you are experiencing difficulties with cross-server sign-in or transfers. See the following sections:

- Users Hear the Opening Greeting Instead of the PIN Prompt When Attempting to Sign In, page 20-17
- Users Hear a Prompt Indicating That Their Home Server Cannot Be Reached During Cross-Server Sign-In, page 20-17
- User ID and PIN Are Not Accepted During Cross-Server Sign-In, page 20-17
- Callers Are Prompted to Leave a Message Rather Than Being Transferred to the Remote User, page 20-18
- Callers Are Transferred to the Wrong User at the Destination Location, page 20-18
- Callers Hear a Prompt Indicating That Their Call Cannot Be Completed When Attempting to Transfer to a Remote User, page 20-19

Users Hear the Opening Greeting Instead of the PIN Prompt When Attempting to Sign In

If a user attempts a cross-server sign-in and hears the opening greeting, the problem may be caused by one of the following:

- The originating location is not configured for cross-server sign-in hand-offs to the destination location. In Cisco Unity Connection Administration on the originating location, confirm that the Allow Cross-Server Sign-In to this Remote Location check box is checked on the Edit Connection Location page for the destination location.
- The user is not found in the search scope on the originating location. Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is trying to sign in. In Cisco Unity Connection Administration on the originating location, check the direct call routing rules to determine which search space is set by the rule that sends calls to the Attempt Sign-In conversation. If the partitions that contain remote users are not a part of this search space, cross-server sign-in does not work, even if it is enabled.

Users Hear a Prompt Indicating That Their Home Server Cannot Be Reached During Cross-Server Sign-In

When a cross-server sign-in hand-off fails to complete successfully, users hear a prompt indicating that their home server cannot be reached at this time. This may happen for one of the following reasons:

- The destination location is not configured to accept cross-server hand-offs. In Cisco Unity Connection Administration on the destination location, confirm that the Respond to Cross-Server Handoff Requests check box is checked on the System Settings > Advanced > Conversations page.
- The Cross-Server Dial String that is defined for the destination location on the originating location is incorrect, or the originating location is unable to place a call to this string by using the phone system integration that is used to dial out. In Connection Administration on the originating location, check the Cross-Server Dial String value on the Edit Connection Location page.
- No ports are available to dial out on the originating location or to answer the call on the destination location. You can use the Connection Port Usage Analyzer to help determine if port usage is becoming a problem for cross-server transfers. You can download the tool and view the Port Usage Analyzer Help at http://www.ciscounitytools.com/App_CUC_PortUsageAnalyzerLL.htm.

User ID and PIN Are Not Accepted During Cross-Server Sign-In

If a user attempts a cross-server sign-in and the call appears to be handed off correctly to the destination location but the user cannot sign in, the most likely cause is that the user is not found in the search scope on the destination location, or another user with an overlapping extension is found first in the search scope.

Cisco Unity Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is trying to sign in, both on the originating and destination locations. In general, we recommend that the same search scope be used by the routing rules that handle cross-server sign-in on both the originating and destination locations. If necessary, you can add a routing rule on the destination location that specifically handles cross-server calls (for example, based on the calling number matching the extension of a port at the originating location).

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

For information on configuring call routing rules and managing partitions and search spaces, see the "Managing Call Routing Tables in Cisco Unity Connection 9.x" and "Managing Partitions and Search Spaces in Cisco Unity Connection 9.x" chapters of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Callers Are Prompted to Leave a Message Rather Than Being Transferred to the Remote User

If callers are prompted to leave a message for a user at the destination location even though the active transfer rule for that user is configured to transfer calls to an extension, this is may be a sign that the cross-server transfer hand-off has failed. This can happen for one of the following reasons:

- The originating location is not configured to perform cross-server transfers to the destination location. In Cisco Unity Connection Administration on the originating location, confirm that the Allow Cross-Server Transfer to this Remote Location check box is checked on the Edit Connection Location page for the destination location.
- The destination location is not configured to accept cross-server hand-offs. In Connection Administration on the destination location, confirm that the Respond to Cross-Server Handoff Requests check box is checked on the System Settings > Advanced > Conversations page.
- The Cross-Server Dial String that is defined for the destination location on the originating location is incorrect, or the originating location is unable to place a call to this string by using the phone system integration that is used to dial out. In Connection Administration on the originating location, check the Cross-Server Dial String value on the Edit Connection Location page.
- No ports are available to dial out on the originating location or to answer the call on the destination location. You can use the Connection Port Usage Analyzer to help determine if port usage is becoming a problem for cross-server transfers. You can download the tool and view the Port Usage Analyzer Help at http://www.ciscounitytools.com/Applications/CxN/PortUsageAnalyzer/PortUsageAnalyzer.html.

Note that if the currently active transfer extension for the user is configured to perform a supervised transfer to an extension that is busy, callers are transferred to voicemail to leave a message when the If Extension Is Busy field is configured to do so, even if the cross-server transfer was successful.

Callers Are Transferred to the Wrong User at the Destination Location

If a caller attempts a cross-server transfer and the call appears to be handed off correctly to the destination location but the caller reaches the wrong user at the destination, the most likely cause is that another user with an overlapping extension is found first in the search scope when the call is passed to the destination.

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Callers Hear a Prompt Indicating That Their Call Cannot Be Completed When Attempting to Transfer to a Remote User

If a caller attempts a cross-server transfer and the call appears to be handed off correctly to the destination location, but the caller hears a prompt indicating that the call cannot be completed and Cisco Unity Connection hangs up, the most likely cause is that the remote user is not found in the search scope when the call is passed to the destination.

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

CHAPTER 21

Troubleshooting Cisco Unity Connection SRSV in Connection 9.1(1)

Added November 27, 2012

Cisco Unity Connection Surviable Remote Site Voicemail is a backup voicemail system that allows you to receive voice messages during WAN outages. See the following sections for information on troubleshooting problems with the Connection SRSV:

Error Message Appears When You Test the Connectivity of Connection with the branch

You may receive the following error messages on the **Edit Branch** page of Cisco Unity Connection Administration when you test the connectivity of Connection with the branch:

- **"Authentication failed. Incorrect Username and Password."**:If you receive the "Authentication failed. Incorrect Username and Password." error message on the **Edit Branch** page when you test the connectivity of the central Connection server with the branch, make sure that the username and password of the branch entered on the Edit Branch page are correct.
- **"Branch is unreachable"**: If you receive the "Branch is unreachable" error message on the **Edit Branch** page when you test the connectivity of the central Connection server with the branch, make sure that the PAT port number specified on the **Edit Branch** page is correct.
- **"Server Address is Invalid"**: If you receive the "Server Address is Invalid" error on the **Edit Branch** page, make sure that the FQDN/IP address of the branch entered on the **Edit Branch** page is correct. In case DNS is configured, make sure that the IP address of the branch is added to it.

Certificate Mismatch Error Appears on the Central Connection Server

If you are getting the "**Unable to start provisioning.**" error on the **Edit Branch** page of Connection Administration page, make sure that the hostname of the branch mentioned in the certificate installed on the central Connection server is correct.

Unable to login to the Cisco Unity Connection SRSV Administration

Connection SRSV Administration gets locked if you enter incorrect administrator username and password of the branch three times on the **Edit Branch** page of Connection Administration. To unlock the Connection SRSV Administration interface, you need to reset the administrator credentials for the branch using the **utilsreset_application_ui_administrator_password** CLI command. For more information on this command refer to the "Utils commands" chapter of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*, Release 9.0(1) at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/9_0_1/CUCM_BK_C3A58B83_00_cucm-cli-reference-guide-90_chapter_01001.html.

Branch User is Unable to Login through Telephony User Interface (TUI)

If a branch user is unable to login through the TUI, check the following:

- Make sure that the PIN entered on the central Connection server is synchronized with the branch through provisioning.
- If the branch user is logging in for the first time through the TUI, make sure that the user has set the PIN at the central Connection server and provisioning is done successfully.

Status of Provisioning Remains In Progress for a long time

If the status of provisioning on Cisco Unity Connection Administration remains "In Progress" for a long time, consider the following:

- Check the network connectivity of the central Connection server with the branch.
- Check whether the central Connection server details are entered correctly on the branch.
- Check whether the **Connection Branch Sync Service** is active on both central Connection server and branch. For more information on the services required for Connection SRSV, refer to the "Managing Cisco Unity Connection Services in Version 9.x" chapter of the *Cisco Unified Serviceability Administration Guide* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.
- Check whether the REST services are active on central Connection server and branch.

Provisioning from the Central Connection Server to the Branch Is Not Working

If the provisioning of the users from the central Connection server to the branch does not work, make sure that the license status at central Connection server is not "Expire". If the license status at central Connection server is "Expire", you need to install the required licenses for the central Connection server to make the license status as "Compliance" and start provisioning. For more information on licensing requirements, refer to the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Status of Provisioning is Partial Success

If the status of the provisioning on the **Branch Sync Results** page is "Partial Success", consider the following:

- Make sure that the name of an administrator on the branch is not same as the name of a subscriber on the central Connection server associated with the branch.
- Make sure that the extension of a call handler at the branch is not used as the extension of a branch user at the central Connection server.
- Make sure that the deleted user on the central Connection server is not used on the branch. For example, if a branch user on Connection is used as operator on Connection SRSV, make sure to change the operator at branch before deleting the user at central Connection server.
- Make sure that the deleted distribution list on the central Connection server is not used on the branch. For example, if a distribution list is used in a call handler template on the branch, make sure to change the distribution list in the template before deleting the distribution list.

Provisioning/Voicemail Upload Remains in Scheduled state for a long time

If the provisioning of the users or voicemail upload remains in the Scheduled state for a long time, make sure that the **Connection Branch Sync Service** is active on the central Connection server.

Unable to Reach a Branch User through Telephony User Interface (TUI)

If you are not able to reach a branch user through TUI, make sure that the associated partition is added in the **Search Space** of the central Connection server.

Unable to Send a Voice Message to a Branch User During WAN Outage

If you are unable to send a voice message to a branch user during WAN outage, make sure that Visual VoiceMail (VVM) is not installed on your phone. For more information, contact your phone service provider.

Error Messages Appear on the Branch Sync Results Page

If the username and password of the branch is not entered correctly on the **Edit Branch** page, the provisioning of the users and the voicemail upload does not work and you will receive the following error messages or status in the **Description** field of the **Branch Sync Results** page of Cisco Unity Connection Administration:

- Unable to start Provisioning of the branch:: Message = Authentication failed.
- Unable to fetch voice mail summary of the branch:: Message = Authentication failed.

If you receive the **"Unable to start provisioning of the branch:: Message=Central Server is not Configured on CUCE"** error message on the **Branch Sync Results** page of Cisco Unity Connection Administration when you start provisioning of the branch, enter the correct FQDN/ IP address of the central Connection server on Cisco Unity Connection SRSV Administration to resolve the problem.

Logs are Not Created or SRSV feature is Not Working Properly

If the logs for the branch are not generated or the SRSV feature is not working properly, you may restart the **Connection Branch Sync Service** and the REST APIs on both the branch and Connection sites to resolve this issue.

Unable to Perform Backup/Restore Operation on the Branch

If you are unable to perform the backup/restore operation on the branch, make sure that the backup server is configured correctly on the branch.

Central Connection Server Moves to Violation State

If the central Connection server moves to the Violation state, make sure that the number of licenses for the Connection features, such as SpeechView and Connection SRSV, does not exceed its maximum limit. For more information on licensing, refer to the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection* Release 9.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Non-Delivery Receipts (NDR) on the Central Connection Server

If you are getting NDR on the central Connection server but the same email is delivered on the branch, check the NDR code and take action accordingly. For example, if user A sends email to user B from the branch, the email gets successfully delivered to user B on the branch. However, on the central Connection server, user A receives "4.2.2" NDR code stating that the mailbox quota of user B has exceeded its maximum limit. In this case, user B needs to take appropriate action, such as delete existing emails or get the mailbax quota increased to receive further emails. For more information on NDR codes, refer to the "Troubleshooting Non-Delivery Receipts in Cisco Unity Connection 9.x" chapter of this guide.

CHAPTER 22

Troubleshooting Notification Devices in Cisco Unity Connection 9.x

Cisco Unity Connection can be configured to call a phone or pager or send text or SMS messages to notify users of new messages and calendar events. See the following sections for information on troubleshooting problems with notification devices:

Message Notifications Through Phones Is Slow for Multiple Users in Cisco Unity Connection 9.x

When message notification through phones is slow for multiple users, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Slow Message Notifications Through Phones for Multiple Users

1. Confirm that ports are not too busy to handle message notification. See the "Ports Are Too Busy to Make Notification Calls Promptly" section on page 22-2.
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 22-2.
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 22-3.

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 small number of ports to exclusively make notification calls.

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

To Review Port Configuration for Message Notification

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

Step 2 On the Search Ports page, review the existing port configuration and determine whether one or more ports can be set to dial out for message notification only.

Not Enough Ports Are Set for Message Notification Only

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

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

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

To Determine Whether the Number of Message Notification Ports Is Adequate

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Reports**.

Step 3 On the Serviceability Reports page, select **Port Activity Report**.

Step 4 On the Port Activity Report page, select the applicable file format for the report output.

Step 5 Set a date range by selecting the beginning and ending month, day, year, and time.

Step 6 Select **Generate Report**.

Step 7 View the report output, depending on the file format that you chose in Step 4.

Step 8 If the port usage during peak periods does not exceed 70 percent, the number of message waiting indication ports is adequate. Skip the remaining steps in this procedure.

If the port usage during peak periods exceeds 70 percent, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 9 On the Search Ports page, review the existing port configuration and determine whether more ports can be set to dial out for message notification only.

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

If the phone system is programmed to send calls to a port on Cisco Unity Connection that is not configured to answer calls, it is possible for a call collision to occur, which can freeze the port.

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

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

Step 2 Note which ports are set to answer calls.

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

Step 4 If you make a change to the phone system programming, in Cisco Unity Connection Administration, select the display name of the port that you changed in Step 3.

Step 5 On the Port Basics page, under Phone System Port, select **Restart**.

Step 6 When prompted that restarting the port will terminate any call that the port is currently handling, select **OK**.

Step 7 Repeat Step 4 through Step 6 for all remaining ports that you changed in Step 3.

Message Notification Is Slow for a User in Cisco Unity Connection 9.x

There are several possible reasons that message notification may appear to be slow for a user. Use the following task list to troubleshoot the possible causes.

Task List for Troubleshooting Slow Message Notification for a Single User

1. The user settings may not be adequate for the needs of the user. See the "Message Notification Setup Is Inadequate" section on page 22-3.
2. The user settings may need adjustment to more correctly map to the work schedule of the user. See the "Notification Attempts Are Missed" section on page 22-4.
3. The user may not clearly understand how repeat notifications are handled by Cisco Unity Connection. See the "Repeat Notification Option Is Misunderstood" section on page 22-5.

Message Notification Setup Is Inadequate

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

To Determine Whether Notification Setup Is Adequate

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, confirm that the notification device is configured to meet the needs of the user. If the user has selected a very busy phone for Connection to call, ask the user if there is an alternate device to use for message notification.

Step 6 In the Related Links list, select **Edit Notification Device Details**, and select **Go**. Verify with the user that the notification schedule that is specified on the Cisco Personal Communications Assistant page is consistent with the days and times that the user is available to receive notification calls.

Notification Attempts Are Missed

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

To Resolve Missed Notification Attempts

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, check the **Repeat Notification If There Are Still New Messages** check box.

Step 6 If the user has another notification device available, for On Notification Failure, select **Send To**, and select the device.

Note Because Connection does not detect notification failure for SMTP devices, the On Notification Failure field is not available for notification devices of this type.

Step 7 For phone or pager notification devices, in the Busy Retry Limit and RNA Retry Limit fields, increase the numbers so that Connection makes more notification calls when the device does not answer or is busy.

Step 8 For phone or pager notification devices, in the Busy Retry Interval and RNA Retry Interval fields, decrease the numbers so that Connection makes notification calls more often when the device does not answer or is busy.

Step 9 Select **Save**.

Step 10 If you chose another device in Step 6, do the following sub-steps:

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

b. On the Notification Devices page, select the display name of the correct notification device.

c. On the Edit Notification Device page, enter settings for the additional device.

d. Select **Save**.

Step 11 For phone notification devices, suggest that the user set up an answering machine for the notification phone, so that notification calls are received even when the user is unavailable.

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

Repeat Notification Option Is Misunderstood

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

To Resolve a Repeat Notification Problem

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, in the Notification Repeat Interval box, set a shorter interval, such as 15 minutes.

Step 6 Select **Save**.

Message Notification Is Not Working at All in Cisco Unity Connection 9.x

There are several possible reasons that message notification may not work at all for a user or group of users. Use the following task list to troubleshoot the possible causes.

Task List for Troubleshooting Non-Functional Message Notifications for a User or Group of Users

- **For all types of notification device:** Confirm that the notification device is enabled and that the notification schedule is set correctly. See the "Notification Device Is Disabled or the Schedule Is Inactive" section on page 22-6.

  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 22-7.

- **For phone or pager notification devices:** Confirm that the message notification phone number is correct and that it includes the access code for an external line if notification is to an external phone. See the "Notification Number Is Incorrect or Access Code for an External Line Is Missing (Phone and Pager Notification Devices Only)" section on page 22-7.

  Confirm that the notification device is assigned to the correct phone system. See the "Notification Device Phone System Assignment Is Incorrect (Phone and Pager Notification Devices Only)" section on page 22-8.

- **For SMS notification devices:** See the "SMS Notifications Are Not Working" section on page 22-9 for additional troubleshooting steps.

- **For SMTP notification devices:** See the "SMTP Message Notification Is Not Working at All for Multiple Users" section on page 22-9 for additional troubleshooting steps.

Notification Device Is Disabled or the Schedule Is Inactive

When you are troubleshooting message notifications, start by confirming that the device is enabled, and that the notification schedule for the device is currently active.

To Verify a Device Status and Schedule

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, confirm that the **Enabled** check box is checked.

Step 6 In the Related Links list, select **Edit Notification Device Details**, and select **Go**. Verify with the user that the notification schedule that is specified on the Cisco Personal Communications Assistant page is consistent with the days and times that the user is available to receive notification calls.

Only Certain Types of Messages Are Set to Trigger Notification

Cisco Unity Connection can be set so that a user is notified only of certain types of messages. For example, if user notification is set up only for urgent voice messages, regular voice messages do not trigger the notification device.

To Change the Message Types That Trigger a Notification Device

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, under Notification Rule Events, verify the selected message types with the user.

Notification Number Is Incorrect or Access Code for an External Line Is Missing (Phone and Pager Notification Devices Only)

If notifications to a phone or pager are not working at all, the user may have entered a wrong phone number for Cisco Unity Connection to call.

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

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

To Verify the Device Phone Number and Access Code for a Phone or Pager Notification Device

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, under Phone Settings, confirm that the correct access code and phone number are entered in the Phone Number field for the device.

If the phone system requires a pause, enter two commas between the access code and the phone number (for example, 9,,5551234).

To Test a Phone or Pager Notification Device

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

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

Step 2 Confirm that the notification device is on.

Step 3 Set up a test phone (Phone 1) for single-line testing. Use a line connected to a port that is set to dial out for message notification.

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

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

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

Notification Device Phone System Assignment Is Incorrect (Phone and Pager Notification Devices Only)

To Verify Notification Device Phone System Assignment

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

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

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

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

Step 4 On the Notification Devices page, select the display name of the correct notification device.

Step 5 On the Edit Notification Device page, under Phone Settings, note the phone system that is specified in the Phone System field.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 7 On the Search Ports page, confirm that the phone system assigned to the notification device has at least one port designated for message notification. Correct the port settings if necessary.

SMS Notifications Are Not Working

If SMS notifications are not working, in Cisco Unity Connection Administration, check the settings on the System Settings > Advanced > SMPP Providers > Edit SMPP Provider page to confirm that the settings match the settings specified by the provider.

If settings on the Edit SMPP Provider page are correct, enable the SMS Device (level 30) micro trace to collect trace information that will help you troubleshoot the problem. For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

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

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

SMTP Message Notification Is Not Working at All for Multiple Users

If SMTP notifications are not working, in Cisco Unity Connection Administration, check the System Settings > SMTP Configuration > Smart Host page to confirm that a smart host is configured. To enable Connection to send text message notifications by using SMTP, your Connection server must be configured to relay messages through a smart host.

If a smart host is already configured on the Smart Host page, note the IP address or host name of the smart host and check to make sure that this smart host is configured to accept messages from the Connection server.

If the smart host settings are configured correctly, you can use traces to track whether the SMTP notification messages are being sent by the Connection server. The default SMTP micro traces (levels 10, 11, 12 and 13) indicate if there is a permanent problem with delivery of a notification message to the smart host. The SMTP micro trace level 18 (Network Messages) shows the details if the notification message is delivered to the smart host. For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Message Notifications Function Intermittently in Cisco Unity Connection 9.x

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

To correct the problem, edit the schedules of the notification devices for the user so that the notification devices are active when the user wants message notifications delivered. You must sign in to the user account in the Cisco Personal Communications Assistant (PCA) to modify the schedule for notification devices.

Cisco Unity Connection Administration does not expose schedules for notification devices. From the Notification Device page for the user in Connection Administration, you can navigate to the Cisco PCA page for the user by selecting the Edit Notification Device Details link in the Related Links list.

For details on using the Cisco PCA, see the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.

Notification Devices Added in Cisco Unity Connection Administration 9.x Are Triggered at All Hours

When a notification device is added for a user in Cisco Unity Connection Administration, by default, the device is active at all times. If a user is receiving notifications at unexpected times, you can modify the notification device schedule to prevent this. You must sign in to the user account in the Cisco Personal Communications Assistant (PCA) to modify the schedule for notification devices.

Connection Administration does not expose schedules for notification devices. From the Notification Device page for the user in Connection Administration, you can navigate to the Cisco PCA page for the user by selecting the Edit Notification Device Details link in the Related Links list.

For details on using the Cisco PCA, see the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 9.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.

Message Notification Received When There Are No Messages in Cisco Unity Connection 9.x

When users are members of a distribution list that is the recipient of a call handler that is configured to mark messages for dispatch delivery, it is possible for a user to receive a message notification for a message that no longer appears in the user inbox when he or she attempts to access it. This can happen because another member of the distribution list has accepted the message between the time that the notification was sent and the time that the user tries to listen to the message.

When configuring message notification rules to include dispatch messages, make users aware that by the time they receive the notification and call in to retrieve the message, it may be gone from their mailboxes because another user has already accepted the message.

For more information on dispatch messages, see the "Dispatch Messages in Cisco Unity Connection 9.x" section in the "Messaging in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

CHAPTER 23

Troubleshooting Non-Delivery Receipts in Cisco Unity Connection 9.x

See the following sections:

Troubleshooting Nondelivery Receipts in Cisco Unity Connection 9.x

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

Cisco Unity Connection 9.x Nondelivery Receipt Status Codes

As you examine a nondelivery receipt (NDR), look for a three-digit code (for example, 4.2.2).

Note that in general, the first decimal place refers to the class of code: 4.x.x is a transient failure and resend attempts may be successful, while 5.x.x is a permanent error.

A more detailed analysis and a list of standard errors for SMTP are available in RFC 1893—Enhanced Mail System Status Codes.

Status codes in Cisco Unity Connection have the following meanings:

- 4.0.0—An unknown error (for example, connectivity problems) prevented Connection from communicating with another SMTP server.
- 4.0.1—Error connecting to the SMTP server.
- 4.0.2—An unknown error (for example, connectivity problems) prevented Connection from communicating with another SMTP server.
- 4.2.1—The recipient mailbox has been dismounted.
- 4.2.2—The recipient mailbox is over the allotted quota set by the administrator.
- 4.2.4 —There is no valid recipient for the message.
- 4.3.2—The message store where the recipient is located has been dismounted.

- 5.1.1—The recipient mailbox cannot be resolved, possibly because the recipient address does not exist or is not correct.
- 5.2.0—An unknown error condition exists, and Connection cannot process the message.
- 5.4.4—There are errors in the VPIM configuration in Connection.
- 5.5.4—There was a permanent error in connecting to the SMTP server.
- 5.6.5—The conversion of a Connection message to a VPIM message failed.
- 5.7.1—A user attempted to send a private message to a contact, which is not supported.
- 5.7.2—An error occurred during expansion of a distribution list.
- 5.7.3—A user attempted to send a secure message to a contact, which is not supported.
- 5.3.10—A fax message failed.

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

CHAPTER 24

Troubleshooting the Cisco Unity Connection 9.x Conversation

See the following sections:

Custom Keypad Mapping Does Not Seem to Take Effect in Cisco Unity Connection 9.x

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

Do the applicable procedure.

To Change the Conversation Style for a Single User

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

Step 2 On the Search Users page, select the alias of the user.

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

Step 3 On the Edit menu, select **Phone Menu**.

Step 4 In the Touchtone Conversation list, select the applicable Custom Keypad Mapping.

Step 5 Select **Save**.

To Specify a Custom Keypad Mapping Conversation for Multiple User Accounts at Once

Step 1 In Cisco Unity Connection Administration, on the Search Users page, check the applicable user check boxes, and select **Bulk Edit**.

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

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

Step 2 On the Edit menu, select **Phone Menu**.

Step 3 In the Touchtone Conversation list, select the applicable Custom Keypad Mapping.

Step 4 If applicable, set the Bulk Edit Task Scheduling Fields to schedule the Bulk Edit operation for a later date and/or time.

Step 5 Select **Submit**.

Long Pauses After Listening to the Help Menu in Cisco Unity Connection 9.x

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

Determining Which WAV File Is Being Played in Cisco Unity Connection 9.x

To determine which WAV file is being played off of the hard disk, do the following procedures in the order given.

To Download the Remote Port Status Monitor

Step 1 In a web browser, go to the Cisco Unity Tools website at http://www.ciscounitytools.com.

Step 2 In the Tool Update Log section, select **Port Status Monitor**.

Step 3 On the Cisco Unified Communication Tools page for the Port Status Monitor, select **Download Now**.

Step 4 Follow the on-screen instructions to download the Remote Port Status Monitor tool.

To Configure Cisco Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Conversations**.

Step 2 On the Conversation Configuration page, check the **Enable Remote Port Status Monitor Output** check box.

Step 3 In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations.

Note that you can enter up to 70 IP addresses, separated by commas.

Step 4 Select **Save**.

To Enable the PhraseServerToMonitor Micro Trace and View the WAV Filename

Step 1 In Cisco Unity Connection Serviceability, on the Trace menu, select **Micro Traces**.

Step 2 On the Micro Traces page, in the Server field, select the name of the Cisco Unity Connection server and select **Go**.

Step 3 In the Micro Trace field, select **PhraseServerToMonitor** and select **Go**.

Step 4 Check the check boxes for all levels and select **Save**.

Step 5 On your workstation, start Remote Port Status Monitor.

Step 6 Make a call to Cisco Unity Connection so that the WAV file is played.

The full path of the WAV files being played appears in the Remote Port Status Monitor window.

Step 7 In Cisco Unity Connection Serviceability, disable the traces that you enabled in Step 3 and Step 4, then select **Save**.

CHAPTER 25

Troubleshooting Voice Recognition in Cisco Unity Connection 9.x

See the following sections for information on troubleshooting problems with the voice recognition conversation:

Users Hear the Phone Keypad Conversation Rather Than the Voice-Recognition Conversation in Cisco Unity Connection 9.x

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

1. Does this problem occur for all users whose accounts are configured for voice recognition? If so, do the following sub-tasks:
   a. Confirm that the class of service (COS) is configured to enable voice recognition. On the Class of Service page, under Licensed Features, check the Allow Access to Advanced Features check box, then check the Allow Users to Use Voice Recognition check box.
   b. Confirm that the affected users are associated with the correct COS.
2. Does this problem occur only for a single user whose account is configured for voice recognition? If so, do the following sub-tasks:
   a. Confirm that the affected user is associated with the correct class of service.
   b. Confirm that the phone menu input style is set to voice recognition. The input style can be set either in the Messaging Assistant web tool or in Cisco Unity Connection Administration.
3. Do users hear a prompt indicating that voice-recognition services are not available when they first sign in?

   If so, see the "Error Prompt: "There Are Not Enough Voice-Recognition Resources"" section on page 25-2.
4. Is the correct codec being used?

Voice recognition does not work if the Connection server or the phone system is using G.729a, if the G.729a prompts are installed, or if greetings and names were recorded in an audio format other than G.711 Mu-Law.

Error Prompt: "There Are Not Enough Voice-Recognition Resources"

When a user hears the error prompt "There are not enough voice-recognition resources at this time. You will need to use the standard touchtones for the duration of this call," do the following tasks in the order presented:

1. Confirm that the Connection Voice Recognizer service is running on the Tools > Service Management page in Cisco Unity Connection Serviceability.

Note For information on Cisco Unity Connection Serviceability, see the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

2. Check the Cisco Unity Connection license on the System Settings > Licenses page in Cisco Unity Connection Administration. It may be that all licensed voice-recognition sessions are being used. If users report that the error occurs frequently, it is likely that voice-recognition usage has outgrown current licensing capacity on your Connection server.
3. Check for errors generated by the Connection Voice Recognizer service. You can use the Real-Time Monitoring Tool (RTMT) to view errors in the diagnostic logs that are generated with the default traces turned on. The trace log filenames are in the format diag_NSSserver_*.uc.

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

Voice Commands Are Recognized, But Names Are Not in Cisco Unity Connection 9.x

When administrators add or change names on the Cisco Unity Connection system, the names are not recognized by the voice-recognition conversation until they are compiled in the grammars. The timing of the grammar compilation can therefore affect name recognition. In other cases, there may be a search scope problem, or the names may not be pronounced the way they are spelled. Use the following troubleshooting steps to determine the source of problem and to correct it:

- Check to make sure that the name is found in the search scope of the user or directory handler, depending on where the recognition problem occurs. The search scope of a user who has signed in is defined on the User Basics page in Cisco Unity Connection Administration. The search scope of a directory handler is defined on the Edit Directory Handler Basics page.
- Check the Voice Recognition Update schedule on the System Settings > Schedules page in Connection Administration; if names have been added during inactive periods in this schedule, they are not recognized until the schedule is active, at which time Connection automatically updates the name grammars.

- Make sure the Connection Voice Recognition Transport service is running on the Tools > Service Management page in Cisco Unity Connection Serviceability.

Note For information on Cisco Unity Connection Serviceability, see the *Administration Guide for Cisco Unity Connection Serviceability Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/serv_administration/guide/9xcucservagx.html.

- Check the Tools > Grammar Statistics page in Cisco Unity Connection Administration to see if a grammar has updates pending. To force an update when a grammar says that updates are pending but does not say it is rebuilding, select the Rebuild Grammars button.
- If the problem occurs in a voice-enabled directory handler, try adjusting the Speech Confidence Threshold setting for the directory handler. A lower speech confidence threshold level results in more matches when callers say names, but when callers say digits, extraneous extension matches are returned. A higher speech confidence threshold level results in more precise extension matching, but fewer name matches.
- If the voice-recognition system is having trouble understanding how a particular name is pronounced, consider adding nicknames or alternate names. You can use both of these features to add differing pronunciations for names that are not pronounced the way they look. (For example, if a username is Janet but is pronounced Jah-nay, you could add the pronunciation "Jahnay" as an alternate name or nickname.)

Note For information on adding nicknames for a user or alternate names for system distribution lists or VPIM locations, see the "Changing Conversation Settings for All Users in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html. See the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html for information on adding alternate names for a user.

Voice Commands Are Not Recognized in Cisco Unity Connection 9.x

When users encounter issues with poor recognition of voice commands, the problem may stem from many sources—the wrong command being used, issues with pronunciation or foreign accent recognition, a poor phone connection, jitter in the network, and so on. Use the following troubleshooting steps to narrow down the source of the problem and to correct it:

1. Determine the nature of the problem.
   a. If the user is having a problem with a single command, see the "Voice Commands" section in the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 9.x)* for a table of preferred voice commands. (The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucu

gphone.html.) Although the voice-recognition grammar files contain many synonyms for the preferred commands, it is not possible for them to contain every word or phrase a user might say. For the best performance, encourage users to use the preferred commands.

b. If the user is having a problem with Connection taking unintended actions without prompting for confirmation, or if Connection is prompting for confirmation too frequently, check the Voice Recognition Confirmation Confidence Threshold setting. See the "Checking the Voice Recognition Confirmation Confidence Setting" section on page 25-4.

2. Try to reproduce the problem while running the Remote Port Status Monitor to determine which voice commands Connection thinks are being uttered. See the "Using the Remote Port Status Monitor" section on page 25-6.
3. Capture and listen to user utterance files to determine if the problem is related to audio quality or accent recognition. See the "Using the Utterance Capture Trace to Review User Utterances" section on page 25-5.
4. Enable diagnostic traces and try to reproduce the problem. See the "Using Diagnostic Traces for Voice Recognition" section on page 25-4.

Checking the Voice Recognition Confirmation Confidence Setting

You can use the Voice Recognition Confirmation Confidence setting to adjust the likelihood that Cisco Unity Connection prompts the voice recognition user to verify certain user intentions. For example, if users complain that the system mistakenly hears them say "cancel" or "hang up," you can try increasing the value of this setting to prevent users from accidentally committing actions they did not intend. Alternatively, if users complain that the system prompts for confirmation too frequently, try adjusting this setting to a lower value.

Voice Recognition Confirmation Confidence is set on a systemwide basis on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration. The setting also can be changed on a per-user basis on the Phone Menu page for an individual user.

A realistic range of values for this setting is 30 to 90. The default value of 60 should reliably filter out most errors and provide confirmation when necessary for most systems.

Diagnostic Tools for Troubleshooting Voice Recognition Problems in Cisco Unity Connection 9.x

There are diagnostic tools available to help you troubleshoot voice-recognition problems. See the following sections:

Using Diagnostic Traces for Voice Recognition

Cisco Unity Connection Serviceability offers diagnostic micro traces and macro traces for help in troubleshooting voice-recognition issues. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Micro Traces

- Conversation Development Environment (CDE)
  - 10 State Machine Trace
  - 22 Speech Recognition Grammar
- Media: Input/Output (MiuIO)
  - 25 ASR and MRCP
- Subscriber Conversation (ConvSub)
  - 03 Named Properties Access
  - 05 Call Progress
- Phrase Server
  - 10 Speech Recognition

Macro Traces

Set the Voice User Interface/Speech Recognition Traces.

Note Use this macro trace only if you have first tried to diagnose the problem by using the recommended micro traces. The macro trace generates a large amount of diagnostic information which can be difficult to sort through.

Using the Utterance Capture Trace to Review User Utterances

When you enable the VUI micro trace level 05 (Capture Utterances), Cisco Unity Connection saves user utterances as WAV files in CCITT (u-law) 8-kHz mono format. The files are stored on the file system, with one folder created for each MRCP session. (You can view MRCP session information for a call in the diagnostic logs by enabling the MiuIO level 25 micro trace for ASR and MRCP.)

You can access the utterance files by using the Real-Time Monitoring Tool (RTMT). Do the following procedure:

Caution Enabling the utterance capture micro trace can affect system performance. Consider doing so only when the system is not under heavy load, and be sure to disable the trace when you are done collecting the desired utterances.

To Enable and View Utterance Capture Traces by Using RTMT

Step 1 In Cisco Unity Connection Serviceability, on the Trace menu, select **Micro Traces**.

Step 2 On the Micro Traces page, in the Server field, select the name of the Connection server and select **Go**.

Step 3 In the Micro Trace field, select **VUI** and select **Go**.

Step 4 Check the **Capture Utterances** check box (level 05) and select **Save**.

Step 5 Reproduce the problem.

Step 6 To access the utterance files, launch Real-Time Monitoring Tool (RTMT). For details, see the "Working with Trace and Log Central" chapter of the *Cisco Unified Real-Time Monitoring Tool Administration Guide, Release 8.0(1)*.

Step 7 In RTMT, on the System menu, select **Tools > Trace > Trace & Log Central**.

Step 8 In the Trace & Log Central tree hierarchy, double-click **Remote Browse**.

Step 9 In the Remote Browse window, select **Trace Files** and select **Next**.

Step 10 In the Select CUC Services/Application tab, check the check box next to the IP address of the server and select **Next**.

Step 11 In the Select System Services/Applications tab, select **Finish**.

Step 12 When the Result pop-up displays, indicating that the Remote Browse is ready, select **Close**.

Step 13 On the Remote Browse tab, browse to the **Nodes > Server Name > CUC > Connection Voice Recognition Transport** folder.

Step 14 In the Connection Voice Recognition Transport folder, double-click the name of a folder to view the audio files that were captured for that MRCP session. (One folder is created for each MRCP session.)

Step 15 In the files pane, double-click the name of an audio file to play it.

Step 16 In the Open With window, select the application you want to use to play the audio file.

If an appropriate audio player is not available in the list, select the **Other** tab at the bottom of the window, browse to the location of an audio player, double-click the name of the audio player executable, and select **Open**. Then select the name of the application you just added.

Step 17 Select **OK**.

Step 18 In Cisco Unity Connection Serviceability, disable the trace that you enabled in Step 3, then select **Save**.

Using the Remote Port Status Monitor

The Remote Port Status Monitor tool is useful for troubleshooting voice-recognition problems because it displays the conversation flow for a call in real time, including speech input and confidence scores, system interpretations of utterances, and changes to the search scope that can affect name and digit interpretation during the course of the call. To use the tool, do the following procedures in order.

To Download the Remote Port Status Monitor

Step 1 In a web browser, go to the Cisco Unity Tools website at http://www.ciscounitytools.com.

Step 2 In the Tool Update Log section, select **Port Status Monitor**.

Step 3 On the Cisco Unified Communication Tools page for the Port Status Monitor, select **Download Now**.

Step 4 Follow the on-screen instructions to download the Remote Port Status Monitor tool.

To Configure Cisco Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Conversations**.

Step 2 On the Conversation Configuration page, check the **Enable Remote Port Status Monitor Output** check box.

Step 3 In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations.

Note that you can enter up to 70 IP addresses. Each IP address must be separated from the following IP address by a comma.

Step 4 Select **Save**.

CHAPTER 26

Troubleshooting Personal Call Transfer Rules in Cisco Unity Connection 9.x

See the following sections:

Cisco Unity Connection Personal Call Transfer Rules Settings Are Unavailable in Cisco Unity Connection 9.x

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

In addition, do the following procedure to confirm that the value of the Region Unrestricted Feature licensing option is set to Yes. If the value is set to No, you cannot use personal call transfer rules, and you cannot use English-United States language. To resolve the problem, install a license in which the feature is enabled, and restart Cisco Unity Connection. (An additional fee might be required to enable the feature. Contact your Cisco account team to obtain the updated license file.) For details, see the "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*.

To Determine the Value of the Region Unrestricted Feature Licensing Option

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

Step 2 Below the License Count table, confirm that the value of US English Usage and Personal Call Routing Rules Allowed (LicRegionIsUnrestricted) is set to **Yes**.

Personal Call Transfer Rules and Destinations in Cisco Unity Connection 9.x

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

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

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

Call Screening and Call Holding Options in Cisco Unity Connection 9.x

If call screening and call holding options are not available in the Personal Call Transfer Rules web tool, use the following information to troubleshoot the possible causes:

- Confirm that the user belongs to a class of service that allows access to the call screening and/or call holding options.

Note Call holding applies only to calls to primary extensions.

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

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

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

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

Problems with the Application of Rules in Cisco Unity Connection 9.x

When rules are not applied as expected, consider the following possible issues:

- **An active rule set has been created but it fails when the user receives a call**—See the "Rules Are Not Applied When a User with Active Rules Receives a Call" section on page 26-3.
- **A rule applies to all incoming calls when the user expected it to be applied only to calls from a specific caller**—Personal call transfer rules can be created without a "From" condition (set up either as "from" or "not from"). When set up this way, the rules are applied to all incoming calls.
- **Rules associated with meetings or calendar entries are not working as expected**—See the "Rules Based on a Meeting Condition Are Not Applied Correctly" section on page 26-4.
- **Rules based on a caller or caller group are not applied correctly**—Phone numbers that have been set for the primary extension, home phone, work phone, or mobile device of a user, or for administrator-defined or user-defined contacts must match the incoming caller ID or ANI. Confirm that the phone number of the caller that is specified in Cisco Unity Connection matches the incoming caller ID or ANI.
- **Rules based on a time condition are not applied correctly**—Confirm that the correct time zone has been selected for the user. In Cisco Unity Connection Administration, on the Edit User Basics page for the user, change the selected time zone if necessary.

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

There are several reasons that a rule set can fail:

- Personal call transfer rules are used only when the active basic rule—the standard, alternate or closed transfer rule—is set to apply personal call transfer rules instead of the basic settings.
- If the rule set is specified for a day of the week, but another rule set is enabled for a date range that includes the current date, the date range rule set takes precedence.
- Transfers to a destination without a complete dialable phone number may fail. If there is no other destination to try, the caller is transferred to voicemail.

Use the following troubleshooting steps to resolve the problem:

- Confirm that the active basic transfer rule is configured to use personal call transfer rules. See the "Configuring Basic Transfer Rules to Use Personal Call Transfer Rules" section on page 26-4.
- Use the Call Transfer Rule Tester to check the validity of the rule. The test tells you which rule is currently being invoked. Based on the results, you may want to reprioritize the rules within the rule set.

Note The rule set that contains the rule that you are testing must be enabled or active in order for the Call Transfer Rule Tester to work.

- Confirm that the destinations for the rule set contain dialable phone numbers, including any outdial access codes required by the phone system.
- On the Rules Settings page, confirm that the Disable All Processing of Personal Call Transfer Rules check box is not checked. When the check box is checked, all rule processing is disabled.

Configuring Basic Transfer Rules to Use Personal Call Transfer Rules

Personal call transfer rules are used only when the active basic rule—the standard, alternate or closed transfer rule—is set to apply personal call transfer rules instead of the basic settings.

To turn on personal call transfer rules for a user, do the following procedure.

Users can also use the Messaging Assistant to configure their basic transfer rules to apply personal call transfer rules.

To Turn On Personal Call Transfer Rules for an Individual User

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

Step 2 On the Search Users page, select the alias of the user for whom you want to turn on personal call transfer rules.

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

Step 3 On the Edit menu, select **Transfer Rules**.

Step 4 In the Transfer Rules table, select the transfer rule that you want to use with personal call transfer rules.

Step 5 On the Edit Transfer Rule page, in the When This Basic Rule Is Active field, select **Apply Personal Call Transfer Rules**.

Step 6 Select **Save**.

Step 7 Repeat Step 3 through Step 6 for each additional transfer rule that you want to use.

Rules Based on a Meeting Condition Are Not Applied Correctly

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

Try the following troubleshooting steps:

- Confirm that the Exchange external service is configured properly. In Cisco Unity Connection Administration, expand Unified Messaging > Unified Messaging Services or System Settings > External Services, and confirm that all settings are correct.
- Confirm that the applicable service is configured as an External Service Account for the user. In Cisco Unity Connection Administration, select Users and search for the user. On the Edit User Basics page, on the Edit menu, select Unified Messaging Accounts or External Service Accounts, and verify settings.

Note See the "Creating Calendar and Contact Integrations in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x* for detailed information on setting up external service accounts.

- Confirm that the Exchange-server and Connection-server clocks are synchronized to the same time source.
- If you believe that the problem is due to newly created calendar appointments, you can get around the 30-minute lag for caching appointments by forcing an immediate caching. See the "Forcing an Immediate Caching of Calendar Appointments" section on page 26-5.
- To permanently change the interval at which Connection caches calendar information, see the "Changing the Interval at Which Cisco Unity Connection Caches Calendar Information" section on page 26-5.

See the "Troubleshooting Calendar Integrations in Cisco Unity Connection 9.0" section on page 6-6 for detailed information on troubleshooting Calendar Integrations.

Forcing an Immediate Caching of Calendar Appointments

Do the following procedure to force Cisco Unity Connection to immediately cache calendar information.

To Force an Immediate Caching of Calendar Appointments

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 Under Optional Services, for the Connection Groupware Caching Service, select **Stop**.

Step 3 After the screen refreshes, for the Connection Groupware Caching Service, select **Start**.

Changing the Interval at Which Cisco Unity Connection Caches Calendar Information

Do the applicable procedure to permanently change the interval at which Cisco Unity Connection caches calendar information:

- To Change the Interval at Which Cisco Unity Connection Caches Calendar Information, page 26-5
- To Change the Interval at Which Cisco Unity Connection Caches Calendar Information), page 26-6

To Change the Interval at Which Cisco Unity Connection Caches Calendar Information

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Unified Messaging Services**.

Step 2 On the Unified Messaging Services Configuration page, in the Calendars: Normal Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner. A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.

Step 3 In the Calendars: Short Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

This setting applies to users who have the Use Short Calendar Caching Poll Interval check box checked on the Edit User Basics page.

Step 4 Select **Save**.

To Change the Interval at Which Cisco Unity Connection Caches Calendar Information)

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **External Services**.

Step 2 On the External Services Configuration page, in the Normal Calendar Caching Poll Interval field, enter the length of time in minutes that Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

A larger number reduces the impact on the Connection server while reducing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner. A smaller number increases the impact on the Connection server while increasing the ability of the server to handle last-minute changes to the Outlook calendar data for users in a timely manner.

Step 3 In the Short Calendar Caching Poll Interval field, enter the length of time (in minutes) that Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

This setting applies to users who have the Use Short Calendar Caching Poll Interval check box checked on the Edit User Basics page.

Step 4 Select **Save**.

Problems with the Transfer All Rule in Cisco Unity Connection 9.x

The following issues can occur when using the Transfer All rule:

- **You are unable to create a Transfer All rule**—You cannot create a Transfer All rule in the Personal Call Transfer Rules web tool. The Transfer All rule can be created only by phone. After the rule has been added by phone, it can be edited in the Personal Call Transfer Rules web tools. Both the destination and duration can be changed in the web tool.
- **The Transfer All rule is not applied as expected**—If the Transfer All rule is not being applied as expected, confirm that the destination number includes any outdial access codes required by the phone system.

Phone Menu Behavior When Using Personal Call Transfer Rules in Cisco Unity Connection 9.x

When phone menus do not behave as expected when using personal call transfer rules, consider the following possible issues:

- **Users cannot change personal call transfer rules by using voice commands—**The voice-recognition feature does not yet support the Personal Call Transfer Rules phone menu options. If users want to use personal call transfer rules, they must temporarily switch to using the phone keypad. They can temporarily switch to using the phone keypad by saying "Touchtone conversation," or by pressing 9 at the Main menu.
- **Phone menu options for personal call transfer rules vary**—Users may notice variations in the phone menus for personal call transfer rules that they hear. Personal Call Transfer Rules phone menu options are built dynamically, and they depend on the existing rule sets and which sets are enabled and active.
- **The phone menu for setting or cancelling call forwarding is unavailable**—See the "Phone Menu Option to Set or Cancel Forwarding All Calls to Cisco Unity Connection Is Unavailable" section on page 26-7.
- **Users notice inconsistencies in how calls are placed through Cisco Unity Connection or dialed directly**—See the "Inconsistent Behavior in Calls Placed Through Cisco Unity Connection and Calls Placed Directly to a User Phone" section on page 26-8.
- **Calls loop during rule processing**—See the "Call Looping During Rule Processing" section on page 26-8.

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

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

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

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

Note See the "Managing the Phone System Integrations in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x* for detailed information about AXL server settings. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

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

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

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

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

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

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

Call Looping During Rule Processing

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

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

- In Cisco Unity Connection Administration, expand Telephony Integrations > Phone System and select the applicable phone system. On the Phone System Basics page, check the Enable for Supervised Transfers check box. The Enable for Supervised Transfers setting causes Connection to detect and terminate call looping conditions so that calls proceed correctly.
- In the Cisco Unity Connection Personal Call Transfer Rules web tool, on the Destinations > View Destinations page, check the Loop Detection Enabled check box for any phone-type destinations to help eliminate call-looping problems with Connection forwarding calls to the mobile phone of the user, and the mobile phone forwarding the calls back to Connection. When the Loop Detection setting is enabled, Connection either transfers the call to the next assigned device (if the user has created a destination group) or transfers the call to voicemail if there are no additional destinations defined.
- Allow Connection to maintain control of calls by setting the value in the Rings to Wait field for rule destinations to be less than the value in the Cisco Unified Communications Manager Forward No Answer Timer field. The Cisco Unified CM Forward No Answer Timer value defaults to 12 seconds. A ring occurs approximately every 3 seconds. Therefore, setting the Rings to Wait value for

Connection destinations to 3 rings allows Connection to maintain control of the call. The supervised transfer initiated by Connection pulls the call back before the loop begins, and attempts to transfer the call to the next destination or to voicemail, as applicable.

Using Diagnostic Traces for Personal Call Transfer Rules in Cisco Unity Connection 9.x

You can use traces to troubleshoot problems with personal call transfer rules. For detailed instructions on enabling and collecting diagnostic traces, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

Enable the following micro traces to troubleshoot personal call transfer rules:

- CCL (levels 10, 11, 12, 13)—Used when accessing calendar information.
- CDE (all levels)—Used in rules-related conversations.
- ConvSub (all levels)—Used when configuring personal call transfer rules settings by phone.
- ConvRoutingRules (all levels)—Used when a rules-enabled user receives a call and while transferring calls between destinations.
- CsWebDav (levels 10, 11, 12, 13)—Used when accessing calendar information.
- RulesEngine (all levels)—Used in rule processing during calls to a rules-enabled user to determine the applicable rule. Also used in determining the applicable rule when using the Rules Tester.

If necessary, enable the following micro traces for the supporting components:

- CDL—Used in rules-related conversations.
- CuGAL—Used in rule processing with a meeting condition and for importing contacts from Exchange.
- MiuCall MiuGeneral—Used in rule processing during calls to a rules-enabled user.
- PhraseServer—Used in rules-related conversations to play prompts.
- Notifier—Used in rule processing when sending SMTP and SMS messages.
- TextToSpeech—Used in rule-settings conversation.

Using Performance Counters for Personal Call Transfer Rules in Cisco Unity Connection 9.x

Do the following procedure to use performance counters for the Personal Call Transfer Rules feature.

To Use Performance Counters for Personal Call Transfer Rules

Step 1 Launch Real-Time Monitoring Tool (RTMT).

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

Step 2 In RTMT, on the System menu, select **Performance > Open Performance Monitoring**.

Step 3 Expand the Connection server.

Step 4 Expand **CUC Personal Call Transfer Rules**.

Step 5 Select the applicable counters:

- Applicable Rule Found—Call resulted in rule processing, and an applicable rule was found.
- Destinations Tried—Number of destinations tried while applying personal call transfer rules.
- PCTR Calls—Call is subject to personal call transfer rules processing: user is assigned to a class of service that has the Personal Call Transfer Rules feature enabled; user is associated with a Cisco Unified CM phone system; and user has enabled personal call transfer rules.
- Rules Evaluated—Number of rules evaluated during rule processing in a call.
- Subscriber Reached—Number of times a user was reached while applying personal call transfer rules.
- Transfer Failed—Number of times a transfer to a destination failed while applying personal call transfer rules.
- Voice Mail Reached—Number of times voicemail was reached while applying personal call transfer rules.

CHAPTER 27

Troubleshooting the Cisco Personal Communications Assistant (PCA) in Cisco Unity Connection 9.x

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

Task List for Troubleshooting Problems with the Cisco Personal Communications Assistant

When the Cisco Personal Communications Assistant fails to operate properly, use the following suggestions to resolve the problem:

- If there is an error message associated with the problem, review the "Cisco PCA Error Messages in Cisco Unity Connection 9.x" section on page 27-2.
- Review the "Users Cannot Access Cisco Personal Communications Assistant Pages in Cisco Unity Connection 9.x" section on page 14-2 to consider the most common reasons why users cannot access the Cisco PCA pages, including use of an incorrect URL, incorrect browser settings, or the presence of unsupported software installed on the workstation.
- If users cannot browse to the Cisco PCA website at all or have trouble accessing the Cisco PCA applications, see the "Troubleshooting User and Administrator Access in Cisco Unity Connection 9.x" chapter for the applicable troubleshooting procedures.
- If the problem is that Media Master does not show up correctly or at all, see the "Troubleshooting the Media Master in Cisco Unity Connection 9.x" chapter.
- If the problem is that the menu bar does not display any text, see the "Missing Text on the Menu Bar in Cisco Unity Connection 9.x (Microsoft Windows Only)" section on page 27-4.
- Confirm that the Tomcat service is running. See the "Verifying That the Tomcat Service Is Running in Cisco Unity Connection 9.x" section on page 27-5.
- Confirm whether appropriate changes have been made in the browser settings to support the locales.

If you cannot resolve the problem and plan to report the problem to Cisco TAC, you will be asked to provide information about your system and about the problem.

Cisco PCA Error Messages in Cisco Unity Connection 9.x

Revised September 25, 2012

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

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

Browser error messages	Browser error messages may indicate that the Cisco PCA failed to install, the user does not have network access to the Cisco Unity Connection server, the browser is not configured correctly, or the user does not have the required security certificate installed (if the Cisco PCA uses SSL connections).
Cisco PCA-specific error messages	Cisco PCA-specific error messages are displayed on the Sign-In page or another Cisco PCA page, and typically indicate problems with user credentials or actions within the Cisco PCA.
Java Plugin error messages	Java Plugin-specific error or warning messages are pop-up alerts that occur on pages that load the Java plugin to integrate the Media Master in a web page. These messages typically appear the first time that the Java plugin is loaded when you navigate to a page that contains the Media Master.
Tomcat error messages	Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the Cisco Unity Connection server. A Tomcat error message usually lists the sequence of application errors. Each exception is followed by a description of what the Tomcat service was attempting to do when the error occurred, and for some exceptions, a message explaining the error is also offered. The "Exception" and "Root Cause" sections in the error message may offer additional information about the problem.

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

- Error Message: "Sign-In Status – Account Has Been Locked."
- Error Message: "Apache Tomcat/<Version> – HTTP Status 500 – Internal Server Error."
- Error Message: "Site Is Unavailable."
- Error Message: "This User Account Does Not Have a Mailbox and Cannot Sign In to the Cisco Personal Communications Assistant. To Use the Cisco PCA, You Must Have an Account with a Mailbox."
- Error Message: "Failed to <Save Message>" While Using PC Microphone in Cisco Unity Connection Administration or Cisco PCA
- Error Message "Access denied" While trying to play recordings through MediaMaster using phone

Error Message: "Sign-In Status – Account Has Been Locked."

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

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

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

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

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

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

Contact Cisco TAC.

Error Message: "Site Is Unavailable."

If users encounter the error message "Site is unavailable," confirm that the Apache Tomcat service is running. See the "Verifying That the Tomcat Service Is Running in Cisco Unity Connection 9.x" section on page 27-5.

Error Message: "This User Account Does Not Have a Mailbox and Cannot Sign In to the Cisco Personal Communications Assistant. To Use the Cisco PCA, You Must Have an Account with a Mailbox."

If a user with valid credentials but who does not have an associated Cisco Unity Connection mailbox attempts to sign in to the Cisco Personal Communications Assistant (PCA), the user receives the error "This user account does not have a mailbox and cannot sign in to the Cisco Personal Communications Assistant. To use the Cisco PCA, you must have an account with a mailbox."

To correct the problem, create an account with a mailbox for the user. As a best practice, we recommend that Cisco Unity Connection administrators do not use the same user account to sign in to Cisco Unity Connection Administration that they use to sign in to the Cisco PCA to manage their own Cisco Unity Connection account.

Error Message: “Failed to <Save Message>” While Using PC Microphone in Cisco Unity Connection Administration or Cisco PCA

While uploading an existing .wav file, or saving a new recorded message as a voice name or greeting using the PC microphone, the user receives an error message for failed operation. For example, if a user is saving a new greeting using PC microphone, the user receives “Failed to Save Greeting” error message. This error message appears if the user is using either the Cisco Unity Connection Administration (CUCA) or the Cisco Personal Communications Assistant (CPCA) web application of Cisco Unity Connection. The following exception also appears in the client side Java Console logs:

> Exception in thread "Timeout guard" java.security.AccessControlException: access denied (java.net.SocketPermission 10.93.231.234:8443 connect,resolve)

To send the recorded message successfully, add the below entry in the client side JRE security profile file, that is commonly named as **java.policy** using the IP address of the Connection server. For a cluster, you may need to add an entry for each of publisher and subscriber.

> permission java.net.SocketPermission "10.93.237.101:8443", "connect,resolve";

If you get a permission error while trying to modify the **java.policy** security profile file, you may need to set the permissions of the file to not inherent permissions from its parent and not be read-only.

Error Message "Access denied" While trying to play recordings through MediaMaster using phone

If a user opens Cisco Personal Communications Assistant (CPCA) through Web Inbox and try to play recordings, the user receives the error "Access Denied". To correct the problem, open Cisco PCA directly in a new window instead of opening through Web Inbox and play the recordings

Missing Text on the Menu Bar in Cisco Unity Connection 9.x (Microsoft Windows Only)

If the menu bar of the Cisco Personal Communications Assistant web tool is missing text and only displays down arrows to signify the menu items, do the following procedure.

To Re-Register DLLs Required for the Cisco Personal Communications Assistant Menu Bar

Step 1 On the user workstation, select **Start** and select **Run**.

Step 2 In Run window, enter **regsvr32 msscript.ocx** and select **OK**.

Step 3 In the dialog box that indicates that the DLL registration succeeded, select **OK**.

Step 4 Select **Start** and select **Run**.

Step 5 In Run window, enter **regsvr32 dispex.dll** and select **OK**.

Step 6 In the dialog box that indicates that the DLL registration succeeded, select **OK**.

Step 7 Select **Start** and select **Run**.

Step 8 In Run window, enter **regsvr32 vbscript.dll** and select **OK**.

Step 9 In the dialog box that indicates that the DLL registration succeeded, select **OK**.

Verifying That the Tomcat Service Is Running in Cisco Unity Connection 9.x

Do the following tasks to confirm that the Tomcat service is running and if necessary, to restart the Tomcat service:

1. Confirm that the Tomcat service is running by using either Real-Time Monitoring Tool (RTMT) or the Command Line Interface (CLI). Do the applicable procedure:
   - To Confirm That the Tomcat Service Is Running by Using Real-Time Monitoring Tool (RTMT), page 27-5
   - To Confirm That the Tomcat Service Is Running by Using the Command Line Interface (CLI), page 27-5
2. If necessary, restart the Tomcat service by using the Command Line Interface (CLI). See the "To Restart the Tomcat Service by Using the Command Line Interface (CLI)" procedure on page 27-5.

To Confirm That the Tomcat Service Is Running by Using Real-Time Monitoring Tool (RTMT)

Step 1 Launch Real-Time Monitoring Tool (RTMT).

Note For details on using RTMT, see the applicable *Cisco Unified Real Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 2 On the System menu, select **Server > Critical Services**.

Step 3 On the System tab, locate Cisco Tomcat and view its status. The status is indicated by an icon.

To Confirm That the Tomcat Service Is Running by Using the Command Line Interface (CLI)

Step 1 Use the Command Line Interface (CLI) command **utils service list** to list all of the services.

Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 2 Scan the CLI output for the Cisco Tomcat service and confirm that its status is **Started**.

To Restart the Tomcat Service by Using the Command Line Interface (CLI)

Step 1 To restart the Cisco Tomcat service, use the CLI command **utils service restart Cisco Tomcat**.

Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

CHAPTER 28

Troubleshooting the Web Inbox in Cisco Unity Connection

The Web Inbox application provides access to voice messages and receipts stored on the Cisco Unity Connection server. The Web Inbox enables users to play, compose, reply to or forward, and manage Connection voice messages by using a web browser. It is installed on the Connection server during installation.

Task List for Troubleshooting Problems with Web Inbox

When the Web Inbox application fails to operate properly, use the following suggestions to resolve the problem:

- If there is an error message associated with the problem, review the "Web Inbox Error Messages in Cisco Unity Connection" section on page 28-2.
- Review the "Users Cannot Access the Web Inbox in Cisco Unity Connection" section on page 28-3 to consider the most common reasons why users cannot access the Web Inbox pages, including use of an incorrect URL, incorrect browser settings, or the presence of unsupported software installed on the workstation.
- If the problem is that the user sees an extra browser window when signing in to Web Inbox, see the "Internet Explorer 7 Users See An Extra Browser Window After Signing in to Web Inbox" section on page 28-4
- If the problem is that the user sees a warning image in lower left side of the browser, see the "Internet Explorer 7 Users See A Warning Image at Lower Left Side of Browser Window After Signing in to Web Inbox" section on page 28-5
- If the problem is that the Adobe Flash Player Settings dialog box appears but no options on the dialog box can be selected, see the "Adobe Flash Player Settings Dialog Box Is Unresponsive (Mac OS X with Firefox Only)" section on page 28-5.
- If the problem is that no messages are displayed in the Web Inbox, see the "Messages Are Not Displayed in the Web Inbox" section on page 28-5.
- If the problem is that users do not see any sent items in the Sent Folder, see the "Sent Messages Are Not Displayed in the Web Inbox" section on page 28-6.
- Confirm that the Tomcat service is running. See the "Verifying That the Tomcat Service Is Running in Cisco Unity Connection" section on page 28-6.
- If the problem is that the Web Inbox does not get open in Internet Explorer 9 with Windows 7 64 bit, see the "Web Inbox Not Working with Internet Explorer 9 on Windows 7 64 bit" section on page 28-7.

If you cannot resolve the problem and plan to report the problem to Cisco TAC, you will be asked to provide information about your system and about the problem.

Web Inbox Error Messages in Cisco Unity Connection

In addition to browser error messages (such as "File not found" or "Unauthorized access"), users may see Web Inbox-specific error messages, Flash plugin error messages, Quicktime plugin error messages, and Tomcat error messages when signing in to or using the Web Inbox.

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

Browser error messages	Browser error messages may indicate that the Web Inbox failed to install, the user does not have network access to the Cisco Unity Connection server, the browser is not configured correctly, or the user does not have the required security certificate installed (if the Web Inbox uses SSL connections).
Web Inbox-specific error messages	Web Inbox-specific error messages are displayed on the Sign-In page or another Web Inbox page, and typically indicate problems with user credentials or actions within the Web Inbox.
Quicktime Plugin error messages	Quicktime Plugin-specific error or warning messages are pop-up alerts that occur on pages that load the Quicktime plugin recording and playback controls. These messages typically appear the first time that the Quicktime plugin is loaded when you navigate to a page that contains the controls.
Tomcat error messages	Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the Cisco Unity Connection server. A Tomcat error message usually lists the sequence of application errors. Each exception is followed by a description of what the Tomcat service was attempting to do when the error occurred, and for some exceptions, a message explaining the error is also offered. The "Exception" and "Root Cause" sections in the error message may offer additional information about the problem.

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

- Error Message: "Sign-In Status – Account Has Been Locked."
- Error Message: "Apache Tomcat/<Version> – HTTP Status 500 – Internal Server Error."
- Error Message: "Site Is Unavailable."
- Error Message: "This User Account Does Not Have a Mailbox and Cannot Sign In to the Web Inbox. To Use the Web Inbox, You Must Have an Account with a Mailbox."

Error Message: "Sign-In Status – Account Has Been Locked."

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

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

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

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

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

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

Contact Cisco TAC.

Error Message: "Site Is Unavailable."

If users encounter the error message "Site is unavailable," confirm that the Apache Tomcat service is running. See the "Verifying That the Tomcat Service Is Running in Cisco Unity Connection" section on page 28-6.

Error Message: "This User Account Does Not Have a Mailbox and Cannot Sign In to the Web Inbox. To Use the Web Inbox, You Must Have an Account with a Mailbox."

If a user with valid credentials but who does not have an associated Cisco Unity Connection mailbox attempts to sign in to the Web Inbox, the user receives the error "This user account does not have a mailbox and cannot sign in to the Web Inbox. To use the Web Inbox, you must have an account with a mailbox."

To correct the problem, create an account with a mailbox for the user. As a best practice, we recommend that Cisco Unity Connection administrators do not use the same user account to sign in to Cisco Unity Connection Administration that they use to sign in to the Web Inbox to manage their own Cisco Unity Connection account.

Users Cannot Access the Web Inbox in Cisco Unity Connection

When a user cannot access the Web Inbox pages, consider the following possible causes.

- The URL is case-sensitive—Users can access the Web Inbox at the following URL: http://<Cisco Unity Connection server>/inbox. Note, however, that the URL is case-sensitive.
- The browser or client is not configured properly—When a user cannot access any of the Web Inbox pages, it may be that the user browser or client workstation is not configured properly. Make sure that the browser and client workstation are configured as specified in the User Workstation Setup Guide for Cisco Unity Connection Release 9.x. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.
- Unsupported software is installed on the client workstation—Confirm that the user does not have an unsupported combination of software or an unsupported third-party application installed on the workstation. See the Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html.

Internet Explorer 7 Users See An Extra Browser Window After Signing in to Web Inbox

When a user sees an extra window (a duplicate of the Web Inbox window, except without the Web Inbox controls displayed above the message area) after signing in to Web Inbox in Internet Explorer 7, do the following procedure to eliminate the extra window.

To Configure Internet Explorer 7 to Eliminate Extra Web Inbox Browser Windows

Step 1 In Internet Explorer 7, select **Tools > Internet Options**.

Step 2 In the Internet Options window, select the **Security** tab.

Step 3 Select the **Internet** zone.

Step 4 In the Security Level for this Zone area, select **Custom Level**.

Step 5 In the Miscellaneous section, locate **Navigate Sub-Frames Across Different Domains**, and select **Enable**.

Step 6 Select **OK** to close the Security Settings window.

Step 7 In the Internet Options window, select the **Local Internet** zone.

Step 8 In the Security Level for this Zone area, select **Custom Level**.

Step 9 In the Miscellaneous section, locate **Navigate Sub-Frames Across Different Domains**, and select **Enable**.

Step 10 Select **OK** to close the Security Settings window.

Step 11 Select **OK** to close the Internet Options window.

Internet Explorer 7 Users See A Warning Image at Lower Left Side of Browser Window After Signing in to Web Inbox

If a user gets a warning image in the lower left side of the browser while logging in Web Inbox using Internet Explorer 7, then the pop-up blocker option must be enabled in the browser.

To Enable the Popup Blocker Option

Step 1 In Internet Explorer 7, select **Tools > Internet Options**.

Step 2 In the Internet Options window, select the **Privacy** tab.

Step 3 In the Pop-up Blocker section, select the TurnOn Pop-up Blocker option.

Step 4 Select **OK** to close the Internet Options window.

Adobe Flash Player Settings Dialog Box Is Unresponsive (Mac OS X with Firefox Only)

When a user presses the record button to compose a message for the first time in the Web Inbox, an Adobe Flash Player Settings dialog box is displayed, asking the user whether to allow the Web Inbox to access the microphone. In some cases, users who see this dialog box are unable to select any of the options in the dialog box, and are therefore unable to record audio for the message. To change the global Flash Player privacy settings so that the dialog box does not appear, do the following procedure.

Note In order to perform this procedure, the user must have access to the Internet to reach the Adobe Macromedia web site.

To Change Global Flash Player Privacy Settings to Allow the Web Inbox to Access the Computer Microphone

Step 1 In the web browser that you use to access the Web Inbox, navigate to the Website Privacy Settings panel of the Adobe Flash Player Settings Manager at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html.

Step 2 In the Adobe Flash Player Settings Manager Website Privacy Settings panel, in the Visited Websites table, locate and select the website corresponding to the Web Inbox.

Step 3 While the Web Inbox site is selected, select **Always Allow** as the privacy setting. When this change is made, Web Inbox can access the computer microphone without prompting the user for permission.

Messages Are Not Displayed in the Web Inbox

If the Web Inbox does not display any messages for a user even though the user has messages in the folder being displayed, clear the browser cache. (Refer to the browser documentation for instructions on how to clear the cache.)

Sent Messages Are Not Displayed in the Web Inbox

In order for sent messages to be available to users in the Sent folder in the Web Inbox, the Sent Messages feature must be enabled. By default, the feature is not enabled. To enable the feature, change the Sent Messages: Retention Period (in Days) setting on the System Settings > Advanced > Messaging page in Cisco Unity Connection Administration to a value greater than zero. Note that because sent messages count toward user mailbox quotas, configuring a high value for this setting can cause user mailboxes to fill with sent messages if users do not regularly manage them from the Web Inbox.

Verifying That the Tomcat Service Is Running in Cisco Unity Connection

Do the following tasks to confirm that the Tomcat service is running and if necessary, to restart the Tomcat service:

1. Confirm that the Tomcat service is running by using either Real-Time Monitoring Tool (RTMT) or the Command Line Interface (CLI). Do the applicable procedure:
   - To Confirm That the Tomcat Service Is Running by Using Real-Time Monitoring Tool (RTMT), page 28-6
   - To Confirm That the Tomcat Service Is Running by Using the Command Line Interface (CLI), page 28-6
2. If necessary, restart the Tomcat service by using the Command Line Interface (CLI). See the "To Restart the Tomcat Service by Using the Command Line Interface (CLI)" procedure on page 28-7.

To Confirm That the Tomcat Service Is Running by Using Real-Time Monitoring Tool (RTMT)

Step 1 Launch Real-Time Monitoring Tool (RTMT).

Note For details on using RTMT, see the applicable *Cisco Unified Real Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 2 On the System menu, select **Server > Critical Services**.

Step 3 On the System tab, locate Cisco Tomcat and view its status. The status is indicated by an icon.

To Confirm That the Tomcat Service Is Running by Using the Command Line Interface (CLI)

Step 1 Use the Command Line Interface (CLI) command **utils service list** to list all of the services.

Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 2 Scan the CLI output for the Cisco Tomcat service and confirm that its status is **Started**.

To Restart the Tomcat Service by Using the Command Line Interface (CLI)

Step 1 To restart the Cisco Tomcat service, use the CLI command **utils service restart Cisco Tomcat**.

Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Web Inbox Not Working with Internet Explorer 9 on Windows 7 64 bit

If the Web Inbox is not working with Internet Explorer 9 on Windows 7 64 bit, make sure that the Media Feature Pack is installed in your system.

CHAPTER 29

Troubleshooting the HTML Notifications in Cisco Unity Connection

Cisco Unity Connection allows you to deliver the SMTP-based HTML notifications for a new voice message to the end users. These notifications can be sent as an HTML format embedded in the email via SMTP. The users get the flexibility to receive the HTML notifications that can include customized icons, header, and footer along with the link to access Cisco Unity Connection Mini Web Inbox. Connection Mini Web Inbox is a player that allows user to play the voice messages over computer or mobile devices.

Ensure that you have taken care of all the requirements and checklist while creating the HTML templates. For more information on the checklist while creating and rendering a template, refer to the "Checklist for Creating and Rendering a Template - Must haves" section in the Adding, Modifying, or Deleting a Notification Template in Cisco Unity Connection 9.x chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* Release 9.x available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

For more information on 'Must Haves' for Cisco Unity Connection Mini Web Inbox, refer to the *Quick Start Guide for the Cisco Unity Connection Mini Web Inbox* available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/quick_start/guide/b_9xcucqsgminiinbox.html.

Note It is recommended, that the Connection Mini Web Inbox must always be opened from the notification email as it requires certain URL parameters.

Task List for Troubleshooting Problems with HTML Notifications and Connection Mini Web Inbox

When the HTML notifications or Connection Mini Web Inbox fail to operate properly, use the following suggestions to resolve the problem

- If the HTML notifications are not received by the users, review "HTML Notifications Are Not Received By the Users, page 29-2" section.
- If the images are not displayed in the email notification on Microsoft Outlook, review the "Images Are Not Displayed on Microsoft Outlook, page 29-2" section.
- If the images are not displayed in the email notification on Internet Explorer 8, review the "Images Are Not Displayed on Internet Explorer 8, page 29-3" section.
- If the images are not displayed in the email notification on IBM Lotus Notes, review the "Images Are Not Displayed on IBM Lotus Notes, page 29-4" section.
- If the hyperlinks are not visible in the email notification, review the "Hyperlinks Are Not Visible in the Email Notification, page 29-4" section.

- If you are not able to launch Connection Mini Web Inbox, review the "Unable to Launch Connection Mini Web Inbox, page 29-4.
- Review the "Unable to View the Updated Cisco Unity Connection Mini Web Inbox Interface in Internet Explorer, page 29-4" section if the user is not able to view the updated Connection Mini Web Inbox window on Internet Explorer.
- If you are not able to play and record messages on computer using Connection Mini Web Inbox, review the "Unable to Play and Record Voice Messages on Computer Using Cisco Unity Connection Mini Web Inbox, page 29-5" section.

HTML Notifications Are Not Received By the Users

If the users are not receiving the HTML notifications, ensure the following steps:

- Confirm that the smart host hostname is configured from Cisco Unity Connection Administration. For more information, refer to the "Setting Up HTML or SMTP Message Notifications in Cisco Unity Connection 9.x" section of the "Setting Up HTML, SMTP, and SMS (SMPP) Message Notifications in Cisco Unity Connection 9.x" chapter of the System Administration Guide for *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- Ping the smart host from Connection server. If the ping fails, there is a possibility that network connection is not functional and you must restore the network connection.
- Confirm that the '**Connection Notifier**' service is up and running.
- Confirm that the HTML notification device is enabled. For more information on how to setup the HTML notification device, refer to the Notification Devices in Cisco Unity Connection 9.x section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
- Confirm that a valid email address is specified while configuring HTML notifications for a user. For more information on how to setup the HTML notification device, refer to the Notification Devices in Cisco Unity Connection 9.x section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Images Are Not Displayed on Microsoft Outlook

If the user is using Microsoft Outlook client for checking the email notifications and is unable to view the images in the notification, do the following steps:

- If the images are not displayed, right click the image and select the **Show Images** options.
- Make sure the minimum requirements for images to be displayed on Microsoft Outlook are met. To check the settings for Microsoft Outlook, refer to the "Configuring Microsoft Outlook to Display Images in an HTML Message Notification" section of the Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages chapter of the *User Workstation Setup Guide for*

Cisco Unity Connection Release 9.x, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

- If the authentication mode is selected, then make sure you are giving the correct credentials.
- If the user enters wrong password thrice continuously then Connection will not prompt the user again and the user must restart the Outlook. To enter the credentials and display the images in the notification you must restart the Outlook.
- When prompted for credentials at the first instance, if the user clicks on the **Cancel** button and does not enter Connection credentials then no image will be displayed in the email notification. You must restart the Outlook to enter the Connection credential and view the images.
- If the images are not getting displayed in the email notification even after installing the required hotfix and Outlook has been restarted, then follow the below mentioned steps:
  1. Check the version of MSO.DLL from the path *C:\Program Files\Common Files\Microsoft Shared\MSORUN* on the Windows machine. Ensure that the version of MSO must include the fix. For more information on version, refer to the details of the Outlook 2007 and Outlook 2010 hotfix.
  2. After restarting Outlook, you must ensure that it is no longer running by ending any running process of Outlook.exe from the Task Manager window. The changes to MSO.DLL will take affect only after proper shutdown and restart of the Outlook.
- Make sure that the registry entry for AllowImageProxyAuth was made for DWORD only.
- If the user is not able to see any images even after all the recommended settings, check the network connectivity of the Connection Server with Internet Explorer by copying the link of the images and manually opening it over the browser.
  - You can check the connectivity via wireshark captures and filtering over SSL packet flow over 443 or 8443 port for the communication.

Images Are Not Displayed on Internet Explorer 8

If the user is using Microsoft Internet Explorer 8 for checking the email notification and unable to view the images, do the following steps:

- Confirm the option to display the images is enabled. For more information refer to "Images Are Not Displayed on Internet Explorer 8" section of the "Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection* Release 9.x, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.
- If the authentication mode is selected, then make sure you are giving the correct credentials. For more information on how to select the authentication mode, refer to the Configuring the Authentication Mode section of the "Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection* Release 9.x, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Images Are Not Displayed on IBM Lotus Notes

If the user is using IBM Lotus Notes for checking the email notification and unable to view the images, do the following steps

- If the images are not displayed, right click the image and select show images options.
- If the authentication mode is selected, then make sure you are giving the correct credentials. For more information on how to select the authentication mode, refer to the Configuring the Authentication Mode section of the "Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection* Release 9.x, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Hyperlinks Are Not Visible in the Email Notification

If the hyperlinks given in the notification template are not visible in the notification, then you need to make sure that the HTML notification template in Cisco Unity Connection Administration has the valid HTML tags and all items (static, action, and status items) are given correctly.

For more information on how to define the tags and the items, refer to the "Adding, Modifying, or Deleting a Notification Template in Cisco Unity Connection 9.x" chapter of the*User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Unable to Launch Connection Mini Web Inbox

If the user is unable to launch the Connection Mini Web Inbox, ensure the following settings:

- Confirm that under COS assigned to the user, Web Inbox is enabled.
- Confirm that the message for which you are opening the Connection Mini Web Inbox is not deleted.
- Confirm that the user is logged in with the valid user name.

Unable to View the Updated Cisco Unity Connection Mini Web Inbox Interface in Internet Explorer

To View the Updated Interface of Connection Mini Web Inbox

Step 1 Open Internet Explorer and then go to **Tools**.

Step 2 In the Internet Options window under the Browsing History section, click **Settings**.

Step 3 In the Temporary Internet Files and History Settings window, select the **Every time I visit the webpage option to check the newer version of stored pages** option.

Step 4 Click **Ok**.

Unable to Play and Record Voice Messages on Computer Using Cisco Unity Connection Mini Web Inbox

If the user is unable to play and record voice messages on computer using Connection Mini Web Inbox, confirm the following:

- Confirm that the outdial number is configured. For more information on how to setup the outdial number and other fields for the HTML notification device, refer to the "Notification Devices in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
- Confirm that the callback number is configured.
- Confirm that the end user answers the phone.

CHAPTER 30

Troubleshooting the Media Master in Cisco Unity Connection 9.x

The Media Master allows you to make and play recordings, either with a phone or with your computer microphone and speakers. The Media Master appears on each page in Cisco Unity Connection Administration on which recordings can be made, and also appears in Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 and in the Messaging Assistant. (The Media Master is not used in Cisco ViewMail for Microsoft Outlook or in the Web Inbox in Connection.)

See the following sections:

Media Master Does Not Display or Function Correctly in Cisco Unity Connection 9.x Applications

Revised 29 August, 2012

The Media Master may not display or function correctly depending on the operating system and/or browser software installed on the client workstation. Consider the following issues:

- Confirm that the browser configuration is correct. See the "Configuring a Web Browser to Access the Cisco PCA in Cisco Unity Connection 9.x" section in the "Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection 9.x" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 9.x* for information on how to set up web browsers on each user workstation to use the Cisco PCA and the web tools. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

- Confirm that the version combinations of Cisco Unity Connection and the software installed on user workstations is supported. See the *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html.
- Some security and VPN software that is installed on the user workstations can cause problems for the Media Master applet. In particular, software that offers personal firewalls can be problematic. If this is the case, work with the software vendor to determine a configuration that allows the Media Master applet to contact the Connection server, or disable or remove the conflicting security and VPN software from the user client workstation.
- If end users experience the browser being unresponsive or crashing when they navigate to a Cisco PCA page that contains the Media Master (for example, a voice message in the Messaging Inbox web tool in Connection 9.0 or a greeting page in the Messaging Assistant web tool), it is likely that an error has been detected by the Java Runtime Environment (JRE).
- If end users experience problem in loading Media Master applet with MAC OS X for Java Runtime Environment (JRE) 6 and later, then you need to install Java7u6MAC port plugin.

  Do the following tasks in the order presented to resolve the issue:

  1. Determine whether the most recent Java version is installed on the workstation by going to http://www.java.com/en/download/help/testvm.xml?ff3. This page automatically tests which Java version is installed and let you know whether there is a more current version available.
  2. If the most recent Java version is not yet installed, download and install it from http://www.java.com. If the problem is still not resolved, continue with Task 3.
  3. Uninstall all versions of Java that are installed on the user workstation, then reinstall the most recent Java version from http://www.java.com.

  For known Java-related issues with Internet Explorer, more information can be found at http://www.java.com/en/download/help/iecrash.xml.

See the applicable sections below for information on known browser issues:

- Apple Safari, page 30-2
- Microsoft Internet Explorer, page 30-2
- Mozilla Firefox, page 30-3

Apple Safari

Apple Safari users are prompted to open a download site to obtain the Java plugin installer the first time that they browse to a Cisco Personal Communications Assistant (PCA) page that should contain the Media Master. After the desired version is downloaded and installed, users may have to sign out of the Cisco PCA, and close and restart the browser software for the plugin to load properly.

Microsoft Internet Explorer

Microsoft Internet Explorer users are prompted to install the Java plugin the first time that they browse to a Cisco Personal Communications Assistant (PCA) page that should contain the Media Master. Users must have local rights to their workstation in order for the Java plugin to install properly. In addition, the user might have to restart the browser for the newly installed plugin to load. If users choose not to install

the Java plugin, they see a message in place of the Media Master stating that support for "application/x-java-applet" is disabled, and pages containing the Media Master pop up one or more alert messages.

Because the Media Master is a Java Applet, and because all Internet Explorer plugins are wrapped into an ActiveX control, users must configure their browsers to download and run ActiveX controls to support automatic plugin installation and to ensure that the Media Master works correctly.

Mozilla Firefox

Mozilla Firefox users are prompted to open a download site to obtain the Java plugin installer the first time that they browse to a Cisco Personal Communications Assistant (PCA) page that should contain the Media Master. After the desired version is downloaded and installed, users may have to sign out of the Cisco PCA, and close and restart the browser software for the plugin to load properly.

For users who use Mozilla Firefox on Red Hat Linux workstations, the J2SE software uses the Advanced Linux Sound Architecture (ALSA) driver to access system sound devices and control playback and recording functionality. Depending on the sound card, playback and recording capabilities may be limited.

Using the Phone for Playback and Recording in the Media Master in Cisco Unity Connection 9.x

The Media Master supports using the phone as a playback and recording device. The phone device is always available to users. Users can configure the phone device by selecting "Playback & Recording" from the Options menu on the Media Master. From the Playback & Recording Options window, users can configure the active phone number for the phone device (the default value is the primary Cisco Unity Connection extension of the user).

The phone device sends requests over the network to the Cisco Unity Connection server to call the active phone number. When the phone answers, the phone device proceeds with either playing back or recording the voice recording. The call can fail for these reasons:

- Either no active phone number value is defined, or it is defined incorrectly.
- The phone system to which the user is assigned does not have any TRAP ports enabled.
- All TRAP-capable ports on the phone system are busy.
- No phone system is designated to handle TRAP connections.
- Security settings or software prevent the Media Master from contacting the Connection server.

Note that using the phone device is the primary way to listen to or to record secure messages, and to review voice recordings in formats that are not supported by the Media Master local device.

If end users are having trouble with using the phone as a playback and recording device in the Media Master, you may want to direct them to one of the following user guides, each of which has a chapter on using the Media Master:

- *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool*
- *User Guide for Accessing Cisco Unity Connection Voice Messages in an Email Application*
- *User Guide for the Cisco Unity Connection Messaging Inbox Web Tool*

Problems with the Phone Device Ringing the Phone for Playback or Recording of a Voice Message

Use the troubleshooting information in this section if the phone device either does not ring the phone, or rings the phone only once for playback or recording of voice messages:

- **Phone numbers of different lengths are configured on the phone system, causing the phone system to wait for additional digits—**If your site uses phone numbers that vary in length (for example, some users have five-digit numbers and others have four-digit numbers) this can cause a slight delay of approximately two seconds before the call is connected.

  The reason for the delay is that the phone system waits to determine that the entire phone number has been dialed before it connects the call.

- **The phone number dialed by the Media Master is not the expected number**—Confirm that the active phone number specified in the Media Master is correct. To do this, check the Active Phone Number value for the Primary Extension or Other Number in the Playback & Recording Options window for the Media Master.

- **The Media Master software is not updated after a Cisco Unity Connection server upgrade**—If the Media Master software is not updated, this is usually caused by the Java plugin not reloading the Media Master files from Cisco Unity Connection, and instead using the locally-cached versions of the files. If this happens, you can manually update the Media Master software. Do the "To Update the Media Master Software" procedure on page 30-4.

- **No phone system is designated to handle TRAP connections**—By default, the first phone system that is integrated with Connection is designated to handle TRAP connections for the Media Master. If this phone system is replaced by another integration, the new phone system might not be designated to handle TRAP connections.

  When a phone system is not designated to handle TRAP connections, the following error appears.

  ```
  Could not establish a phone conversation.
  The server reports the following:
  Code: 26
  Description: Cannot find a switch to route the call
  ```

  Do the "To Designate a Phone System to Handle TRAP Connections" procedure on page 30-5.

To Update the Media Master Software

Step 1 Close all browser windows.

Step 2 Depending on your operating system, do one of the following:

- For Windows 2000 and later, start the Java control panel by selecting **Start > Settings > Control Panel > Java**.
- For Red Hat Linux and Mac OSX, start the Java control panel found in $JAVA_HOME\bin\ControlPanel.

Step 3 On the General page, under Temporary Internet Files, select **Delete Files**.

This clears the cached files. The Media Master resource files will be downloaded the next time you visit a Cisco PCA or Cisco Unity Connection Administration page that contains the Media Master.

To Designate a Phone System to Handle TRAP Connections

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

Step 2 On the Search Phone Systems page, select the name of the phone system that you want to handle TRAP connections.

Step 3 On the Phone System Basics page, check the **Default TRAP Switch** check box and select **Save**.

Problems Opening a File in the Media Master When It Was Saved on a Workstation in Cisco Unity Connection 9.x

When you attempt to use a previously recorded WAV file (for example, an announcement that was recorded earlier) rather than making a new recording by using a phone or a computer microphone, the Media Master may display the following error message:

> Could not load audio recording from file. The file is either not an audio file, a supported audio format, or is corrupted.

This error occurs when the WAV file was recorded in the G.729a audio format.

To resolve this problem, do one of the following:

- Convert the WAV file to another audio format (for example, convert it to the G.711 audio format).
- Use a WAV file that is recorded in a supported audio format other than G.729a.
- Make the recording by using a phone or a computer microphone.

Note that when Cisco Unity Connection is configured to record in the G.729a audio format, the Media Master functions correctly for recording and playing recordings by using a phone or a computer microphone.

CHAPTER 31

Troubleshooting Phone View in Cisco Unity Connection 9.x

The Phone View feature is supported only with Cisco Unified Communications Manager phone system integrations.

The Phone View feature may not function correctly outside a firewall or through a VPN router.

Requirements for Phone View are available in the "Requirements for Cisco Unity Connection Phone View" section of *System Requirements for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html.

See the following sections:

Problems with Phone View in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if an error message appears when the user attempts to use Phone View. Consider the following possible causes:

- The application user is configured incorrectly. See the "Application User Is Configured Incorrectly" section on page 31-1.
- The user phone configuration is not correct. See the "User Phone Configuration Is Not Correct" section on page 31-2.
- The phone system integration is configured incorrectly. See the "Phone System Integration Is Configured Incorrectly" section on page 31-2.

Application User Is Configured Incorrectly

The problem may be caused by the incorrect configuration of the application user on the Cisco Unified Communications Manager server.

Do the following procedure to verify the configuration of the application user.

To Verify the Configuration of the Application User

Step 1 In Cisco Unified Communications Manager Administration, on the User Management menu, select **Application User**.

Step 2 On the Find and List Application Users page, select **Find**.

Step 3 Select the user ID of the application user that is used by Phone View.

Step 4 On the Application User Configuration page, under Application User Information, select **Edit Credential**.

Step 5 On the Credential Configuration page, confirm that the following check boxes are checked:

- **User Must Change at Next Login**
- **Does Not Expire**

Step 6 Select **Save**.

Step 7 In the Related Links box, select **Back to User** and select **Go**.

Step 8 On the Application User Configuration page, under Application User Information, in the Password field, reenter the password.

Step 9 In the Confirm Password field, reenter the password.

Step 10 Under Device Information, in the Controlled Devices field, confirm that the devices that are associated with the application user account are correct.

Step 11 Select **Save**.

Step 12 On the System menu, select **Enterprise Parameters**.

Step 13 On the Enterprise Parameters Configuration page, under Phone URL Parameters, in the URL Authentication field, confirm that the URL is correct.

Step 14 If you made any changes, select **Save**.

User Phone Configuration Is Not Correct

One possible cause may be that the configuration on the user phone is not current. You can reboot the phone so that it reloads the configuration from the Cisco Unified CM server.

Another possible cause is that the user phone is not supported. See the "Requirements for Cisco Unity Connection Phone View" section of *System Requirements for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html.

Phone System Integration Is Configured Incorrectly

The problem may be caused by the incorrect configuration of the Cisco Unified CM phone system integration in Cisco Unity Connection Administration.

Do the following procedures.

To Verify the Configuration of the Cisco Unified Communications Manager Phone System Integration

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

Step 2 On the Search Phone Systems page, select the name of the phone system.

Step 3 On the Phone System Basics page, under Phone View Settings, confirm that the **Enable Phone View** check box is checked.

Step 4 In the CTI Phone Access Username field, confirm that the name of the application user in Cisco Unified CM Administration is correct.

Note that the name of the application user is case-sensitive.

Step 5 In the CTI Phone Access Password field, reenter the password of the application user in Cisco Unified CM Administration.

Step 6 Select **Save**.

To Verify the Configuration of the User

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

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

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

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

Step 4 On the Phone Menu page, under Finding Messages with Message Locator, confirm that the **Enable** check box is checked.

Step 5 Confirm that the **Enable Phone View** check box is checked.

Step 6 Select **Save**.

Using Traces to Troubleshoot Phone View Issues in Cisco Unity Connection 9.x

You can use traces to troubleshoot Phone View issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Diagnostic Traces in Cisco Unity Connection 9.x" chapter.

CHAPTER 32

Troubleshooting SNMP in Cisco Unity Connection 9.x

Cisco Unity Connection supports Simple Network Management Protocol (SNMP) to provide standard network management. Connection SNMP uses the SNMP Master Agent service in Cisco Unified Serviceability and the Connection SNMP Agent service in Cisco Unity Connection Serviceability.

Note Connection SNMP supports CISCO-UNITY-MIB from Cisco Unity.

See the following sections:

Problems with SNMP in Cisco Unity Connection 9.x

Use the troubleshooting information in this section if you experience problems with SNMP. See the following possible issues:

SNMP Master Agent Service Is Not Running

The SNMP Master Agent service in Cisco Unified Serviceability runs as the master agent. Do the following procedure to confirm that the service is running.

To Confirm That the SNMP Master Agent Service Is Running

Step 1 In Cisco Unified Serviceability, on the Tools menu, select **Control Center - Network Services**.

Step 2 On the Control Center – Network Services page, under Platform Services, confirm that the status of the SNMP Master Agent service is **Started**.

Step 3 If the status is not Started, select **SNMP Master Agent** and select **Restart**.

Connection SNMP Agent Service Is Not Running

The Connection SNMP Agent service in Cisco Unity Connection Serviceability runs as a subagent. Do the following procedure to confirm that the service is running.

To Confirm That the Connection SNMP Agent Service Is Running

Step 1 In Cisco Unity Connection Serviceability, on the Tools menu, select **Service Management**.

Step 2 On the Control Center – Feature Services page, under Base Services, confirm that the Connection SNMP Agent service status is **Started**. If the service status is Stopped, select **Start**.

SNMP Community String Is Configured Incorrectly

The SNMP community string must be configured for SNMP to function correctly. Do the following procedure to confirm that the SNMP community string is configured correctly.

To Confirm That the SNMP Community String Is Configured Correctly

Step 1 In Cisco Unified Serviceability, on the SNMP menu, select **V1/V2 > Community String**.

Step 2 On the SNMP Community String Configuration page, select **Find**.

Step 3 If an SNMP community string appears, select the name. If there is no SNMP community string, select **Add New**.

Step 4 Enter any applicable settings and verify the settings.

Step 5 Select **Save**.

Step 6 When prompted that the SNMP Master Agent service will be restarted, select **OK**.

Using Traces to Troubleshoot SNMP Issues in Cisco Unity Connection 9.x

You can use traces to troubleshoot SNMP issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the "Traces in Cisco Unity Connection Serviceability in Cisco Unity Connection 9.x" section on page 2-1.

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W