# CONTENTS

## CHAPTER 1

**Troubleshooting Cisco Unity Connection** 1

- Troubleshooting Cisco Unity Connection 1
- Using Diagnostic Traces for Troubleshooting 1
- Traces in Cisco Unity Connection Serviceability 1
  - Micro Traces for Selected Problems 2
  - Macro Traces for Selected Problems 12
  - Using Micro or Macro Traces 15
- Traces in Cisco Unified Serviceability 16
  - Traces for Selected Problems 16
  - Using Traces to Troubleshoot Problems 17

## CHAPTER 2

**Troubleshooting Utilities** 19

- Grammar Statistics Tool 19
- Cisco Unity Connection Serviceability 20
- Task Management Tool 20
  - Accessing the Task Management Tool 20
- Cisco Voice Technology Group Subscription Tool 21
- Real-Time Monitoring Tool 21
- Cisco Unified Serviceability 21
- Remote Database Administration Tools 22
- Cisco Utilities Database Link for Informix (CUDLI) 22
- Remote Port Status Monitor 22
- Application Audit Logging 22
- Network Analyzer 23
- System Restore Tool 23
  - Database Error While Creating Restore Point 23
Troubleshooting Cisco Unity Connection Deployments 25

- Troubleshooting Installation Issues 25
- Troubleshooting Upgrade Issues 26
- Troubleshooting Locale Issues After Upgrade 26
- Troubleshooting SELinux Issues 26

Troubleshooting User and Administrator Access 29

- Unity Connection Not Responding to Key Presses 29
  - Enabling DTMF Relay 29
  - Verifying DTMF settings 30
- Users Do Not Hear Sign-in or Desired Prompt When Calling Unity Connection 30
  - Using Port Status Monitor 30
- Administration Accounts Unable to Sign-In to Cisco Unity Connection Serviceability 31
- User Account is Locked over TUI/VUI Interface 31
- User Account is Disabled over Web Applications 31
- Troubleshooting Sign-in Problems with Visual Voicemail (Pin Based Authentication) 32
- Troubleshooting Sign-in Problems with Visual Voicemail (Password Based Authentication) 32
- Error Message Appears While Updating the Phone PIN through Cisco Unity Connection Administration or Cisco PCA 33
- User Display Name Not Get Updated after AD Synchronization 33

Troubleshooting Call Transfers and Call Forwarding 35

- Troubleshooting Call Transfers and Call Forwarding 35
  - Calls Not Transferred to the Correct Greeting 35
    - Confirm that Forward Timer in the Phone System is in Synch with the Rings to Wait For Setting in Unity Connection 36
    - Synchronizing the Forward Timer and the Rings to Wait For Setting 36
    - Confirm that Phone System Integration Enables Playing the User Personal Greeting for Callers 37
  - Verifying the Phone System Integration Settings 37
  - Confirming that Busy Greeting is Supported and Enabled 37
  - Confirming that Search Scope Configuration Sends Call to Intended Destination 38
Problems with Call Transfers (Cisco Unified Communications Manager Express SCCP Integrations Only) 38
Configuring the SCCP Integration for Cisco Unified Communications Manager Express 38
User Hears a Reorder Tone When Answering a Notification Call 39
Correcting the Rings to Wait For Setting 39
Troubleshooting Directory Handler Searches 39
Users Not Found in the Search Scope of Directory Handler 40
Troubleshooting Message Addressing 40
Users Unable to Address Desired Recipients 40
Users Unable to Address a System Distribution List 41
Unexpected Results Returned When a User Addresses by Extension 41
Caller is Not Getting Prompt in Expected Language 41
Using Traces to Determine the Search Space Used During a Call 42

### Chapter 6

#### Troubleshooting Messages

User Hears Full Mailbox Warnings 43
Nondelivery Receipt (NDR) Not Received for Undelivered Message 44
Messages Are Delayed 44
Messages Are Not Delivered 44
User Has a Full Mailbox 45
Undeliverable Messages Not Forwarded to Recipients 46
Users Assigned to Unity Connection Entities Deleted and No Replacements Assigned 46
Unity Connection Unable to Relay Messages 46
Unable to Play Message Audio in Outlook Web Access 47
Unable to Receive Notification Emails for Quota Overflow 47

### Chapter 7

#### Troubleshooting Unified Messaging

Troubleshooting Unified Messaging 49
Troubleshooting Single Inbox Issues 49
Mismatch of Date and Time for Messages in Unity Connection and Exchange 2003 49
Message Relay Not Working or is Not Working as Expected 49
Single Inbox Not Working for Anyone on Unity Connection 50
Single Inbox Not Working for Unified Messaging Users 50
Single Inbox is Not Working for a User or a Subset of Users 54
Single Inbox Synchronization from Exchange is Delayed  56
Single Inbox Synchronization from Office 365 is Delayed  56
Single Inbox Synchronization from Exchange Failed  57
Single Inbox Fails with Office 365 Using ADFS  57
Duplicate Message Issue with Single Inbox  57
Resolving SMTP Domain Name Configuration Issues  58
Troubleshooting Problems with Cisco ViewMail for Microsoft Outlook  58
Voice Messages or Receipts are Not Received in the Outlook Inbox  58
Messages Sent from a Single Inbox Outlook Client are Not Received  59
Messages Received in an Email Account Other than the Single Inbox Account  59
Messages cannot be Played in Outlook  59
Messages Moved into a .PST Folder in Outlook cannot be Played  60
Playing a Message Does Not Turn Off the Message Waiting Indicator  60
Message Waiting Indicator Turns Off Before the Message is Played  61
Deleting a Message in Outlook Does Not Delete the Corresponding Message  61
Messages Moved into a .PST Folder in Outlook are Deleted  61
Troubleshooting Problems with Invalid Passwords  61
Changing a Cisco ViewMail for Microsoft Outlook Password  62
Collecting Diagnostics from ViewMail for Outlook on the User Workstation  62
Enabling Cisco ViewMail for Microsoft Outlook Diagnostics and View the Log Files on the User Workstation  62
Collecting Diagnostics on the Unity Connection Server for Problems with Single Inbox and ViewMail for Outlook  63
Troubleshooting Access to Emails in an External Message Store  63
User on the Phone Hears “Invalid Selection” after Pressing Seven  63
Enabling User Access to Email in an External Message Store  63
User on the Phone Hears “Your Messages are Not Available” after Pressing Seven  63
Users Hear Gibberish at the End or Beginning of an Email  65
Email Deleted by Phone is Still in the Inbox Folder (Exchange 2003 Only)  65
Using Traces to Troubleshoot Access to Emails in an External Message Store  65
Troubleshooting Calendar Integrations  65
Using Unified Messaging Accounts are Used for Calendar Integrations  65
Testing the Calendar Integration  66
Obtaining Unified Messaging Account Status  66
Test Fails the Last Check 66
Test Succeeds but the Calendar Integration Still Does Not Work (Exchange 2003 Only) 67
Non-Published Meetings Do Not Appear in List of Meetings (Cisco Unified MeetingPlace Only) 68
Configuring the Unity Connection Service Account (Cisco Unified MeetingPlace Only) 68
Meetings Do Not Appear in List of Meetings 68
“Access Exchange Calendar and Contacts” Option Not Available for Unified Messaging Accounts 69
Using Traces to Troubleshoot a Calendar Integration 69
Troubleshooting Access to Calendar Information Using Personal Call Transfer Rules 69
Changing the Interval Unity Connection Waits to Update Calendar Information 70
Troubleshooting the Test Button for Unified Messaging Services and Unified Messaging Accounts 70

CHAPTER 8 Troubleshooting IMAP Clients and ViewMail for Outlook 71
Troubleshooting IMAP Clients and ViewMail for Outlook 71
Troubleshooting Problems with Changing Passwords 71
Troubleshooting Sign-In Problems with IMAP Email Clients (LDAP is Not Configured) 71
Troubleshooting Sign-In Problems with IMAP Email Clients (When LDAP is Configured) 72
Troubleshooting Sign-In Problems with IMAP Clients 73
Unable to Login to IMAP Client 73
Messages Sent from an IMAP Client Not Received 73
Checking the IP Address Access List 74
Messages are Received in an Email Account Instead of a Voice Mailbox 75
Voice Messages Not Received in an IMAP Account 75
Intermittent Message Corruption When Using ViewMail for Outlook 76
Recording or Playback Devices Not Appearing in ViewMail Account Settings in ViewMail for Outlook 76
Unable to Play Messages through ViewMail for Outlook 8.5 and Later 76
User Email Account Does Not Appear in ViewMail Options in ViewMail for Outlook 76
ViewMail for Outlook Form Does Not Appear 76
Collecting Diagnostics from ViewMail for Outlook on the User Workstation 77
Enabling ViewMail for Outlook Diagnostics and View the Log Files on the User Workstation 77
Collecting Diagnostics from ViewMail for Outlook on the User Workstation 77
CHAPTER 9

Troubleshooting Non-Delivery Receipts 79

Troubleshooting Non-Delivery Receipts 79

Overview 79

Non-Delivery Receipt Status Codes 79

CHAPTER 10

Troubleshooting Transcription (SpeechView) 81

Troubleshooting Transcription (SpeechView) 81

Task List for Troubleshooting SpeechView 81

Issues Related to Basic Configuration Settings 81

Issues with a Proxy Server 82

Issues with the Transcription Service Configuration 82

Issues Related to User Expectations 83

Issues with Transcription Notifications 83

Enabling Traces and Contacting Cisco TAC 83

Confirming that Connection SpeechView Processor and Connection SMTP Server Services are Running 83

Running SMTP Test to Verify Outgoing and Incoming SMTP Path 84

Troubleshooting Transcription Notifications 85

Messages that Cannot be Transcribed 85

Transcription Not Synchronized on User Phones 86

Using Diagnostic Traces to Troubleshoot SpeechView 86

CHAPTER 11

Troubleshooting Networking 87

Troubleshooting Networking 87

Troubleshooting Intersite Networking Setup 87

"Unable to Contact the Remote Site" Error When Manually Creating an Intersite Link on the Unity Connection Site Gateway 87

"Hostname Entered Does Not Match That on The Remote Site Certificate" Error When Manually Creating an Intersite Link on the Unity Connection Site Gateway 88

Enabling ViewMail for Outlook Diagnostics and View the Log Files on the User Workstation 77

Collecting Diagnostics on Unity Connection for IMAP Client Problems 78

Login via IMAP Fails for LDAPS if IP Address of LDAP Server is Configured 78
"Unable to Link to the Specified Remote Site. Cause: Failed to Assess the Current Network Size"
Error When Creating an Intersite Link on the Unity Connection Site Gateway 89
"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 Unity Connection Site Gateway 89
Troubleshooting HTTPS Networking Setup 89
Unable to Link to Network Location. Cause: Location is Already Part of the network.” Error When Creating an HTTPS Link on Unity Connection” 89
Unable to Link to Network Location. Cause: Publisher (IP Address/FQDN/Hostname) Entered does not Match that on Remote Location Certificate 90
Troubleshooting Directory Synchronization between Two Unity Connections in HTTPS networking 90
Troubleshooting HTTPS Networking Cases 91
Distribution Lists and the Members of the Distribution Lists Not Replicating in HTTPS network 91
How to Synchronize Selective Objects from HTTPS link 91
How to Synchronize Selective Objects, Voice Names of a Specific Location in HTTPS Networking 93
How to Swap Extensions in HTTPS Networking 94
How to Remove Orphan Objects from Unity Connection HTTPS network 95
Received RTMT NetworkLoopDetected 96
Sender Receives NDR When Sending Voice Message to Distribution List 96
Troubleshooting Message Addressing 96
Users Cannot Address Messages to Remote Users, Contacts, or System Distribution Lists 96
Cisco Unity Users Cannot Address Messages to Unity Connection Users or System Distribution Lists 98
Unity Connection Users Cannot Address Messages to Recipients at a VPIM Location 99
Unity Connection Users Cannot Blind Address Messages to a Mailbox at a VPIM Location 100
Troubleshooting Message Transport 100
Messages Sent from Users on One Unity Connection Location Not Received by Users on Another Unity Connection Location 100
Replies to Messages Sent by Remote Senders Not Delivered 101
Messages Sent from a VPIM Location Not Received by Unity Connection Users 101
Messages Sent from Unity Connection Not Received by Users at a VPIM Location 102
Troubleshooting Directory Synchronization 102
Troubleshooting Directory Synchronization Within a Unity Connection Site 102
Troubleshooting Directory Synchronization Between Two Unity Connection Sites 104
Troubleshooting Directory Synchronization Between a Unity Connection Site and a Cisco Unity Site 105

Cross-Server Sign-In and Transfers 107

Users Hear the Opening Greeting Instead of PIN Prompt When Attempting to Sign-In 107
Users Hear a Prompt Indicating that their Home Server Cannot be Reached During Cross-Server Sign-In 107
User ID and PIN Not Accepted During Cross-Server Sign-In 108
Callers Prompted to Leave a Message Instead of Being Transferred to the Remote User 108
Callers Transferred to the Wrong User at the Destination Location 109
Callers Hear a Prompt Indicating that Call Cannot be Completed When Attempting to Transfer to a Remote User 109

Chapter 12

Troubleshooting Cisco Unity Connection SRSV 111

Troubleshooting Cisco Unity Connection SRSV 111
Error Message Appears When Testing the Connectivity of Unity Connection with Branch 111
Certificate Mismatch Error Message for Appears on the Central Unity Connection Server 111
Unable to login to Cisco Unity Connection SRSV Administration 112
Branch User is Unable to Login through Telephony User Interface (TUI) 112
Status of Provisioning Remains In Progress for a Long Time 112
Provisioning from the Central Unity Connection Server to Branch Not Working 112
Status of Provisioning is Partial Success 112
Provisioning/Voicemail Upload Remains in Scheduled state for a Long Time 113
Unable to Reach a Branch User through Telephony User Interface (TUI) 113
Unable to Send a Voice Message to a Branch User During WAN Outage 113
Error Messages Appear on the Branch Sync Results Page 113
Logs are Not Created or SRSV feature Not Working Properly 113
Unable to Perform Backup/Restore Operation on the Branch 114
Central Unity Connection Server Moves to Violation State 114
Non-Delivery Receipts (NDR) on the Central Unity Connection Server 114

Chapter 13

Troubleshooting Video Messaging 115

Troubleshooting Video Messaging 115
Error Message Appears When You Test the Connectivity of Video Services 115
CHAPTER 14  Troubleshooting the Phone System Integration  121

Troubleshooting the Phone System Integration  121
Diagnostic Tools  121
   Configuring Unity Connection for the Remote Port Status Monitor  121
   Using the Check Telephony Configuration Test  122
Troubleshooting Call Control  122
Unity Connection Not Answering Any Calls  122
   Verifying the Phone System Settings in Cisco Unity Connection Administration  122
Unity Connection Not Answering Some Calls  123
   Confirming Routing Rules  123
   Confirming Voice Messaging Port Settings  123
   Confirming that Voice Messaging Ports are Enabled  124
Troubleshooting an Integration of Unity Connection with Cisco Unified Communications Manager  125
   Viewing or Editing IP Address of Cisco Unified Communications Manager  125
   Ports Do Not Register or Repeatedly Disconnected in an SCCP Integration  125
   Ports Do Not Register in an IPv6 Configuration  128
   Determining the Correct Port Group Template  130
   Problems Faced When Unity Connection is Configured for Cisco Unified Communications Manager Authentication or Encryption  130
   Troubleshooting PIN Synchronization between Unity Connection and Cisco Unified CM  137

CHAPTER 15  Troubleshooting Message Waiting Indicators (MWIs)  139
Troubleshooting Message Waiting Indicators (MWIs) 139

Triggers for Turning MWIs On and Off 139

MWI Problems 140

MWIs Do Not Turn On or Off 140
MWIs Turn On but Do Not Turn Off 142
Delay for MWIs to Turn On or Off 144
No Message Count Sent on Phone When MWI is On 145
Incorrect Message Count and False MWI Notification Sent on Phone 145

Troubleshooting Audio Quality 147

Troubleshooting Audio Quality 147

Troubleshoot Audio Quality Using Check Telephony Configuration Test 147
Using the Check Telephony Configuration Test to Troubleshoot Audio Quality 147
Problem with Choppy Audio 147
Problem with Garbled Recordings 148

Troubleshooting a Garbled Audio Stream in the Network 148
Troubleshooting How Unity Connection Makes Recordings 148

Problem with Garbled Prompts on Phone 149
Problem with Volume of Recordings 149

Changing the Volume for Unity Connection Recordings 150
Disabling Automatic Gain Control (AGC) for Unity Connection 150
Confirming the Advertised Codec Settings 150

Using Traces to Troubleshoot Audio Quality Issues 151

Troubleshooting Notification Devices 153

Troubleshooting Notification Devices 153

Overview 153

Message Notifications through Phones is Slow for Multiple Users 153
Ports Too Busy to Make Notification Calls Promptly 153
Not Enough Ports Set for Message Notification Only 154
Confirm that Phone System Sends Calls to the Ports Set to Answer Calls 154
Message Notification Slow for a User 155
Message Notification Setup is Inadequate 155
Notification Attempts are Missed 155
Repeat Notification Option is Misunderstood  156
Message Notification Not Working at All  157
  Notification Device Disabled or the Schedule Inactive  157
  Only Certain Types of Messages Set to Trigger Notification  157
  Notification Number Incorrect or Access Code for an External Line Missing (Phone and Pager Notification Devices Only)  158
  SMS Notifications Not Working  159
  SMTP Message Notification Not Working at All for Multiple Users  160
HTML Notifications Not Working  160
HTML Summary Notification Not Working  160
Message Notifications Function Intermittently  160
Notification Devices Added in Unity Connection Administration Triggered at All Hours  161
Message Notification Received When No Unread Messages  161

Chapter 18  Troubleshooting Comet Notifications over SSL  163
  Troubleshooting Comet Notifications over SSL  163
  Unable to Send Comet Notification over SSL  163

Chapter 19  Troubleshooting a Cisco Unity Connection Cluster Configuration  165
  Troubleshooting a Cisco Unity Connection Cluster Configuration  165
  One Server Stops Functioning and the Other Server is Not Handling Calls  165
    Verifying the Status of the Voice Messaging Ports  166
    Verifying the Voice Messaging Ports Assignments for Phone System Integration  166
    Confirming that Voice Messaging Ports are Registered (SCCP Integrations Only)  166
  Both Servers Attain Primary Server Status  166
  Unity Connection Cluster Not Functioning Correctly  167
    Confirming that Applicable Services are Running on the Server with Primary Server Status  167
    Confirming that Applicable Services are Running on Both Servers  167
  Server Cannot be Added to the Unity Connection Cluster  168
  Cannot Access Alert Logs When the Publisher Server Stops Functioning  168
    Enabling the Subscriber Server to Access the Alert Logs When the Publisher Server Stops Functioning  168

Chapter 20  Troubleshooting Licensing  171
Troubleshooting Licensing  171
Troubleshooting Problems with Licenses  171
Licensing Problems  171
License Violation Status Appears on Cisco Unity Connection Administration  171
Loss of Connectivity Warning Appears on Cisco Unity Connection Administration for Publisher Server  172
Loss of Connectivity Warning Appears on Cisco Unity Connection Administration for Subscriber Server  172
Unity Connection Not Answering Calls  172
Unity Connection Not Answering Calls After License Status Changes from “Expire” to “Compliance”  172
SpeechView Services are Not Working  172

CHAPTER 21

Troubleshooting Voice Recognition  173
Troubleshooting Voice Recognition  173
Users Hear the Phone Keypad Conversation Instead of Voice-Recognition Conversation  173
Error Prompt: There Are Not Enough Voice-Recognition Resources  174
Voice Commands Recognized But Names Not Recognized  174
Voice Commands Not Recognized  175
Checking the Voice Recognition Confirmation Confidence Setting  176
Diagnostic Tools for Troubleshooting Voice Recognition Problems  176
Using Diagnostic Traces for Voice Recognition  176
Using the Utterance Capture Trace to Review User Utterances  177
Using the Remote Port Status Monitor  178

CHAPTER 22

Troubleshooting the Conversation  179
Troubleshooting the Conversation  179
Custom Keypad Mapping Not Taking Effect  179
Changing the Conversation Style for a Single User  179
Specifying a Custom Keypad Mapping Conversation for Multiple User Accounts at Once  179
Long Pauses After Listening to Help Menu  180
Determine the WAV File Played  180
Downloading the Remote Port Status Monitor  180
Configuring Unity Connection for the Remote Port Status Monitor  180
Enabling the Phrase Server To Monitor Micro Trace and View the WAV Filename 180

CHAPTER 23 Troubleshooting SAML SSO Access 181

Troubleshooting SAML SSO Access 181

Redirection to IdP fails 181
IdP authentication fails 181
Redirection to Unity Connection fails 181
Run Test Fails 182
Mismatch in SAML Status on Publisher and Subscriber Servers 182
Problem in Accessing Web Application on Unity Connection 182
Encryption Error Upon User Login to Unity Connection 183
Unable to Upload Subscriber SP Metadata on ADFS in Cluster 183
SAML Exception Time Synchronization Error 184
Incorrect status of SAML SSO on Two Servers in a Unity Connection Cluster 184
Troubleshooting Cross Origin Resource Sharing 184
Diagnostics Traces for Problems with SAML SSO Access 184

CHAPTER 24 Troubleshooting Fax 187

Troubleshooting Fax 187

Problems with Fax Delivery to Users 187
Confirming that SMTP Server Configuration is Correct 188
Confirming that POP3 Mailbox Name and Password are Correct 188
Confirming Fax is Delivered to Unity Connection 188
Problems with Fax Delivery to a Fax Machine 188
Determining the Status of a Fax Delivered to a Fax Machine 189
Confirming that POP3 Mailbox Name and Password are Correct 189
Confirming that SMTP Server Configuration is Correct 189
Confirming that Faxable File Types List is Correct 190
Problems with Fax Notifications 190
Confirming that Fax Notification is Enabled for the User 190
Problems with Fax Receipts 190
Fax Receipts Not Delivered 190
User Mailbox is Filled with Fax Notifications 192
Problems with Printing Faxes 192
CHAPTER 25
Troubleshooting Reports 193

Overview 193

Confirming Connection Reports Data Harvester Service is Running 193

Adjusting Report Data Collection Cycle 194

CHAPTER 26
Troubleshooting Cisco Personal Communications Assistant (PCA) 195

Overview 195

Users cannot Access Cisco PCA Pages 196

Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages 196

Adding the SSL Certificate to the Trusted Root Store on User Workstations 197

Users cannot Access Unity Connection Web Tools from Cisco PCA 197

Users cannot Save Changes on Pages in Cisco PCA 197

Cisco PCA Error Messages 197

Error Message: “Sign-In Status – Account Has Been Locked.” 198


Error Message: “Site is Unavailable.” 199

Error Message: “Failed to <Save Message>” While Using PC Microphone in Cisco Unity Connection Administration or Cisco PCA 199

Error Message: “Application Blocked by Security Settings. Your security settings have blocked a self-signed application from running” 200

Error Message “Access denied” When Trying to Play Recordings through Media Master Using Phone 200

Missing Text on the Menu Bar (Microsoft Windows Only) 200

Re-Registering DLLs Required for the Cisco Personal Communications Assistant Menu Bar 200

Verifying if Tomcat Service is Running 201

Confirming That the Tomcat Service Is Running Using Real-Time Monitoring Tool (RTMT) 201

Confirming That the Tomcat Service Is Running Using the Command Line Interface (CLI) 201

Restarting the Tomcat Service Using the Command Line Interface (CLI) 202

CHAPTER 27
Troubleshooting Personal Call Transfer Rules 203

Troubleshooting Personal Call Transfer Rules 203
Troubleshooting Web Inbox

Introduction

Web Inbox Error Messages

Error Message: “Sign-In Status – Account Has Been Locked.”


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: “Error While Uploading Message to Server”

Error Message: "HTML5 audio compatible browser or QuickTime Plug-in not found. Select Phone option to play the message. Install Quick time plugin or open web inbox into firefox”

Send Option is Disabled on MAC Operating System

Adobe Flash Player Settings Dialog Box Unresponsive (Mac OS X with Firefox Only)

Changing Global Flash Player Privacy Settings to Allow the Web Inbox to Access the Computer Microphone

Messages Not Displayed in Web Inbox
Contents

CHAPTER 29

Troubleshooting the HTML Notifications 219

HTML Notifications Not Received By the Users 219
Images Not Displayed on Microsoft Outlook 220
Images Not Displayed on IBM Lotus Notes 221
Hyperlinks Not Visible in the Email Notification 221
Unable to Launch Mini Web Inbox 221
Unable to View the Updated Mini Web Inbox Interface in Internet Explorer 221
Unable to Play and Record Voice Messages on Computer Using Mini Web Inbox 222

CHAPTER 30

Troubleshooting Custom Roles 223

Troubleshooting Custom Roles 223
Unable to Configure Custom Role 223
Getting "Not Authorized" Error Message on Role Assignment or Unassignment 223
Getting "Not Authorized" Error on Cisco Unity Connection Administration Pages 224

APPENDIX A

Troubleshooting Tenant Partitioning 225

Troubleshooting Issues while Deleting Tenant 225
Users of One Tenant are Able to Send Messages to Users of Other Tenants 226
Able to Hear the Opening Greeting Without being Asked for the PIN 226
Getting Option to Select Users from Other Partitions in Directory Result 227
Debugging Steps 227
Tenant Creation Fails with an Error Message "Non-Tenant users exist on Unity Connection" 227
Troubleshooting Problems While Integrating with Call Manager 228
Hearing the Fast Busy Tone on Dialing the Pilot Number 228
Hearing the Error Message - "The system is temporarily unable to complete your call" on Dialing the Pilot Number 228
Troubleshooting Problems with Migration 229

Sent Messages Not Displayed in Web Inbox 217
Verifying that Tomcat Service is Running 217
Confirming that the Tomcat Service is Running Using Real-Time Monitoring Tool (RTMT) 217
Confirming that the Tomcat Service is Running Using the Command Line Interface (CLI) 218
Restarting the Tomcat Service Using the Command Line Interface (CLI) 218
Web Inbox Not Working with Internet Explorer 9 on Windows 7 64 bit 218
"Mailbox could not be loaded" Error Shows Up 229
SMTP Proxy Address Not Updated on Unity Connection for One or More Subscribers After Migration 229
Hearing a Wrong Post Greeting Recording for Users Belonging to a Tenant 230
Getting Incorrect Time for Incoming or Outgoing Messages 230
Get Incorrect Language for the Incoming or Outgoing Users 230

APPENDIX B

Troubleshooting Phone View 231
Problems with Phone View 231
Application User Configured Incorrectly 231
User Phone Configuration Not Correct 232
Phone System Integration Configured Incorrectly 232
To Verify the Configuration of the Cisco Unified Communications Manager Phone System Integration 232
To Verify the Configuration of the User 233
Using Traces to Troubleshoot Phone View Issues 233

APPENDIX C

Troubleshooting MediaMaster 235
Media Master Does Not Display or Function Correctly in Unity Connection Applications 235
Apple Safari 236
Microsoft Internet Explorer 236
Mozilla Firefox 236
Using the Phone Device for Playback and Recording in Media Master 236
Updating the Media Master Software 238
Designating a Phone System to Handle TRAP Connections 238
Problems Opening a File in the Media Master When Saved on a Workstation 238

APPENDIX D

Troubleshooting Media Player (Release 11.5 (1) and later) 239
Troubleshooting Media Player (Release 11.5 (1) and later) 239
Using the Phone Device for Playback and Recording in Media Player 239
Designating a Phone System to Handle TRAP Connections 240
Problem Uploading a File in the Media Player 240
Unknown Error Appears while Using Media Player 241
<table>
<thead>
<tr>
<th>APPENDIX E</th>
<th>Troubleshooting SNMP</th>
<th>243</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Problems with SNMP</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>To Confirm That the SNMP Master Agent Service Is Running</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>Connection SNMP Agent Service Not Running</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>SNMP Community String Configured Incorrectly</td>
<td>244</td>
</tr>
<tr>
<td></td>
<td>Using Traces to Troubleshoot SNMP Issues</td>
<td>244</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPENDIX F</th>
<th>Troubleshooting Multi-Server Certificate</th>
<th>245</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initial Debugging and Identifying Topology Details</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Initial Debugging</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Collecting Log Files</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>CLI commands to List and Get Log Files</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Required Log Files</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>CLI Commands examples</td>
<td>246</td>
</tr>
</tbody>
</table>
Troubleshooting Cisco Unity Connection

The Troubleshooting Guide for Cisco Unity Connection helps resolve problems that you might encounter with Cisco Unity Connection. If your Unity 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 procedure mentioned in this chapter to determine whether the problem is caused by SELinux Security policies. (SELinux replaced Cisco Security Agent(CSA) on Unity Connection servers.) You can also use traces to troubleshoot various problems associated with Unity Connection.

For more information on the CLI commands, see the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions at.

- Troubleshooting Cisco Unity Connection, on page 1

Troubleshooting Cisco Unity Connection

Using Diagnostic Traces for Troubleshooting

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 using Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

Traces in Cisco Unity Connection Serviceability

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

<table>
<thead>
<tr>
<th>Cisco Unity Connection Serviceability micro traces</th>
<th>Used to troubleshoot problems with specific Unity Connection components.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unity Connection Serviceability macro traces</td>
<td>Used to troubleshoot general areas of Unity Connection functionality.</td>
</tr>
</tbody>
</table>

After the traces are enabled, you can access the trace log files using the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).
## Micro Traces for Selected Problems

You can use Cisco Unity Connection Serviceability micro traces to troubleshoot problems with specific Unity Connection components. Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems provides information on different 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 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/serv_administration/b_11xcucservag.html).

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

### Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audio Issues</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Playing an attachment via the TUI</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>ConvSub (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td><strong>Calendar Integration Issues</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calendar integration</td>
<td>CCL (levels 10, 11, 12, 13)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CsWebDav (levels 10, 11, 12, 13)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Calendar integration (event notifications)</td>
<td>CsWebDav (levels 10 through 13)</td>
<td>Connection IMAP Server</td>
<td>diag_CulmapSvr_*.uc</td>
</tr>
<tr>
<td><strong>Call Issues</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Routing rules</td>
<td>Arbiter (levels 14, 15, 16)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>RoutingRules (level 11)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td><strong>Client Issues</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Personal Communicator client (IMAP-related issues)</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CsMalUmss (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CulmapSvr (all levels)</td>
<td>Connection IMAP Server</td>
<td>diag_CuImapSvr_*.uc</td>
</tr>
<tr>
<td></td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td>ViewMail for Outlook (sending and receiving messages)</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CsMalUmss (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CulmapSvr (all levels)</td>
<td>Connection IMAP Server</td>
<td>diag_CuImapSvr_*.uc</td>
</tr>
<tr>
<td></td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td>Unity Connection Cluster Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unity Connection clusters (except file replication)</td>
<td>SRM (all levels)</td>
<td>Connection Server Role Manager</td>
<td>diag_CuSrm_*.uc</td>
</tr>
</tbody>
</table>

Troubleshooting Guide for Cisco Unity Connection Release 11.x
<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unity Connection cluster file replication</td>
<td>CuFileSync (all levels)</td>
<td>Connection File Syncer</td>
<td>diag_CuFileSync_*_.uc</td>
</tr>
<tr>
<td>External Message Store Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accessing emails in an external message store</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*_.uc</td>
</tr>
<tr>
<td>Fax Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File rendering</td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td>SMTP messages are not sent</td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td>SMTP server mishandles faxes</td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*_.uc</td>
</tr>
<tr>
<td>LDAP Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP synchronization</td>
<td>CuCmDbEventListener</td>
<td>Connection CM Database Event Listener</td>
<td>diag_CuCmDbEventListener_*_.uc</td>
</tr>
<tr>
<td>(see also “LDAP synchronization” in Table 3: Cisco Unified Serviceability Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dispatch messages</td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td>(see also “Dispatch messages” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>IMAP messages (see also “IMAP messages” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*_.uc</td>
</tr>
<tr>
<td></td>
<td>CsMalUmss (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*_.uc</td>
</tr>
<tr>
<td></td>
<td>CulmapSvr (all levels)</td>
<td>Connection IMAP Server</td>
<td>diag_CulmapSvr_*_.uc</td>
</tr>
<tr>
<td></td>
<td>MTA (all levels)</td>
<td>Unity Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td></td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*_.uc</td>
</tr>
<tr>
<td>Message delivery and retrieval (see also “Message delivery and retrieval” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*_.uc</td>
</tr>
<tr>
<td></td>
<td>CsMalUmss (levels 10, 14, 18, 22, 23, 26)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*_.uc</td>
</tr>
<tr>
<td></td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td></td>
<td>Notifier (all levels except 6 and 7)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*_.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*_.uc</td>
</tr>
<tr>
<td></td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*_.uc</td>
</tr>
<tr>
<td></td>
<td>UmsSysAgentTasks (all levels)</td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*_.uc</td>
</tr>
<tr>
<td>Message Relay Issues</td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*_.uc</td>
</tr>
<tr>
<td></td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*_.uc</td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>NDRs</td>
<td>CML (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>(see also “NDRs” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>CuCsMgr (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Notifications not sent</td>
<td>CuCsMgr (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>(see also “Notifications not sent” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td></td>
<td>Notifier (all levels except 6 and 7)</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>Notifier (all levels except 6 and 7)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*.uc</td>
</tr>
<tr>
<td>SMTP/HTML notification/Intelligent Notification</td>
<td>Notifier (all levels except 6 and 7)</td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td>Secure message aging</td>
<td>UmssSysAgentTasks (all levels)</td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*.uc</td>
</tr>
<tr>
<td>SMS notifications</td>
<td>Notifier (all levels except 6 and 7)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
<td></td>
</tr>
<tr>
<td>Networking Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrasite Networking replication</td>
<td>CuReplicator</td>
<td>Connection Digital Networking Replication</td>
<td>diag_CuReplicator_*.uc</td>
</tr>
<tr>
<td>(see also “Intrasite Networking replication” in Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems)</td>
<td></td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Intersite Networking replication</td>
<td>Feeder (levels 00, 01, 02, 03)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>FeedReader (levels 00, 01, 02, 03, 10, 14)</td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*.uc</td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>HTTP(S) Networking</td>
<td>FeedReader (levels 00, 01, 02, 03, 04, 05)</td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*.uc</td>
</tr>
<tr>
<td></td>
<td>Feeder (levels 00, 01, 02, 03)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>VPIM message delivery</td>
<td>MTA (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td>(see also “VPIM message delivery” in Table 2:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unity Connection Serviceability Macro</td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*.uc</td>
</tr>
<tr>
<td>Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Call Transfer Rule Issues</td>
<td>Accessing calendar information</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CsWebDav (levels 10, 11, 12, 13)</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConvSub (all levels)</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Configuring personal call transfer rule settings</td>
<td></td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>by phone</td>
<td></td>
<td>RulesEngine (all levels)</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Rule processing during calls to a rules-enabled</td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Rules-related conversations</td>
<td></td>
<td>RulesEngine (all levels)</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Phone View Issues</td>
<td></td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Phone View</td>
<td>PhoneManager (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Report Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data collection in reports</td>
<td>ReportDataHarvester (all levels)</td>
<td>Connection Report Data Harvester</td>
<td>diag_CuReportDataHarvester_*.uc</td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Display of reports</td>
<td>CuService (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>RSS Feed Issues</td>
<td>RSS (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>SNMP Issues</td>
<td>CuSnmpAgt (all levels)</td>
<td>Connection SNMP Agent</td>
<td>diag_CuSnmpAgt_*.uc</td>
</tr>
<tr>
<td>SpeechView Transcription Issues</td>
<td>SttClient (all levels)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td></td>
<td>SttService (all levels)</td>
<td>Connection SpeechView Processor</td>
<td>diag_SttService_*.uc</td>
</tr>
<tr>
<td></td>
<td>SMTP (all levels)</td>
<td>Connection SMTP Server</td>
<td>diag_SMTP_*.uc</td>
</tr>
<tr>
<td></td>
<td>MTA (level 10, 11, 12, 13)</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td></td>
<td>SysAgent (level 10, 11, 12, 16)</td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*.uc</td>
</tr>
<tr>
<td></td>
<td>Notifier (level 16, 21, 25, 30)</td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td>Test Button (External Service and External Service Account) Issues</td>
<td>CuESD (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Web Inbox Issues</td>
<td>VMREST (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Jabber VoiceMail Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Jabber VoiceMail</td>
<td>Not Applicable as it is enabled by default</td>
<td>Cisco Tomcat</td>
<td>localhost_access_log.txt</td>
</tr>
<tr>
<td></td>
<td>Not Applicable as it is enabled by default</td>
<td>Connection Jetty</td>
<td>request.log</td>
</tr>
<tr>
<td></td>
<td>Notifier (level 18 and 21)</td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td></td>
<td>Cuca</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>VMREST</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Visual VoiceMail Issues</td>
<td>TRAP - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>VMREST (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*._uc</td>
</tr>
<tr>
<td></td>
<td>Arbiter - (level 12 to 17)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>CDE-04 - &lt;13-17&gt;</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>MiuCall - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._ucCu</td>
</tr>
<tr>
<td></td>
<td>MiuGeneral - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>MiuIO - &lt;11-15&gt;</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>MiuMethod - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>MiuSIP - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>MiuSIPStack - (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*._uc</td>
</tr>
<tr>
<td></td>
<td>Mixer - (all levels)</td>
<td>Connection Mixer</td>
<td>diag_CuMixer_*._uc</td>
</tr>
<tr>
<td>Licensing Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td>CuLicMgrSvr (all levels)</td>
<td>Connection License Manager Server</td>
<td>diag_CuLicSvr_<em>._uc elm-client</em>.log</td>
</tr>
<tr>
<td>Tenant Partitioning Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Tenant Partitioning</td>
<td>Cuca</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td>VMREST (all levels)</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Video Greetings Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Greetings</td>
<td>CDE (level 1, 10 to 17, 20, 21)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>ConvSub (level 01 to 05)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>MiuIO (level 11 to 13, 25, 27)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>Miu Sip/Miu Sip Stack (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>MiuMethods/MiuCall (all levels)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>Mixer (levels 01 to 04)</td>
<td>Connection Mixer</td>
<td>diag_CuMixer_*.uc</td>
</tr>
<tr>
<td></td>
<td>Video (level 10 and 11)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>SAML SSO Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML SSO</td>
<td>CLI Command to activate SAML SSO logs: admin: set samlttrace level &lt;trace-level&gt; where trace-level can be BEBUG, INFO, WARNING, ERROR, or FATAL CLI Command to check trace level: admin: show samlttrace level</td>
<td>Cisco Tomcat Cisco Tomcat Security Cisco SSO</td>
<td>ssosp*.log ssoApp.log</td>
</tr>
<tr>
<td>Miscellaneous Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synchronization traces</td>
<td>CsMbxSync</td>
<td>Connection Mailbox Sync</td>
<td>diag_CuMbxSync_*.uc</td>
</tr>
</tbody>
</table>

Troubleshooting Guide for Cisco Unity Connection Release 11.x
## Troubleshooting Cisco Unity Connection

### Micro Traces for Selected Problems

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange EWS calls in MbxSync diag</td>
<td>CsEws</td>
<td>Connection Mailbox Sync</td>
<td>diag_CuMbxSync_<em>.</em>.uc</td>
</tr>
<tr>
<td>EWS notification in Jetty web service diags</td>
<td>EWSNotify</td>
<td>Connection Jetty</td>
<td></td>
</tr>
<tr>
<td>Exchange 2003 webdav protocol diags</td>
<td>CsWebDav</td>
<td>Connection Mailbox Sync</td>
<td>diag_CuMbxSync_*.uc</td>
</tr>
<tr>
<td>Activities of Connection external service</td>
<td>CuEsx</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Message deposition on Connection</td>
<td>MTA</td>
<td>Connection Message Transfer Agent</td>
<td>diag_CuMta_*.uc</td>
</tr>
<tr>
<td>CUCA test buttons for UM service and UM user pages</td>
<td>Cuca</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td>Autodiscovery feature diags</td>
<td>MbxLocator</td>
<td>Connection Mailbox Sync</td>
<td>diag_CuMbxSync_*.uc</td>
</tr>
<tr>
<td>MbxSyncQ and EWSNotifQ events</td>
<td>DBEvent</td>
<td>Connection DB Event Publisher</td>
<td>diag_DbEventPublisher_*.uc</td>
</tr>
</tbody>
</table>

### PIN Synchronization Issues

<table>
<thead>
<tr>
<th>PIN Synchronization Issues</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Synchronization Issues</td>
<td>AxlAccess (level 00,01)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Bulk Administration Tool (all levels)</td>
<td>Tomcat Logs</td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>CiscoPCA (level 00,01,02,13)</td>
<td>Tomcat Logs</td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>Cuca (all levels)</td>
<td>Tomcat Logs</td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>CuCsMgr (level 10)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
<td></td>
</tr>
<tr>
<td>VMREST (all levels)</td>
<td>Tomcat Logs</td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>CDL (level 10 and 11)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
<td></td>
</tr>
<tr>
<td>ConvSub (level 01,03,04,05)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
<td></td>
</tr>
</tbody>
</table>
Macro Traces for Selected Problems

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

Table 2: Cisco Unity Connection Serviceability Macro Traces for Selected Problems 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 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/serv_administration/b_11xcucservag.html).

Note

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

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio quality</td>
<td>Media (Wave) Traces</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Mixer</td>
<td>diag_CuMixer_*.uc</td>
</tr>
<tr>
<td>Call Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call control</td>
<td>Call Control (Miu) Traces</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td>(expand the macro trace to select SIP or SCCP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call flow</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>ViewMail for Outlook</td>
<td>Call Control (Miu) Traces</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>(recording or playback by phone)</td>
<td>(expand the macro trace to select SIP or SCCP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Personal Communicator client (IMAP-related issues) (see also “Cisco Unified Personal Communicator client (IMAP-related issues)” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ViewMail for Outlook (sending and receiving messages)</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>ViewMail for Outlook (see also “ViewMail for Outlook (sending and receiving messages)” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection IMAP Server</td>
<td></td>
<td>diag_CuImapSvr_*.uc</td>
<td></td>
</tr>
<tr>
<td>Connection Message Transfer Agent</td>
<td></td>
<td>diag_MTA_*.uc</td>
<td></td>
</tr>
<tr>
<td>Connection Tomcat Application</td>
<td></td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>Connection REST Service</td>
<td></td>
<td>diag_Tomcat_*.uc</td>
<td></td>
</tr>
<tr>
<td>Connection Mailbox Sync</td>
<td></td>
<td>diag_CuMbxSync_*.uc</td>
<td></td>
</tr>
</tbody>
</table>

Cisco Unity Connection Serviceability Issues

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unity Connection Serviceability</td>
<td>Connection Serviceability Web Service</td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
</tbody>
</table>

Conversation Issues

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversations</td>
<td>Conversation Traces</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
</tbody>
</table>

Message Issues

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatch messages (see also “Dispatch messages” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>IMAP messages (see also “IMAP messages” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>Problem Area</td>
<td>Traces to Set</td>
<td>RTMT Service to Select</td>
<td>Trace Log Filename</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Message delivery and retrieval</td>
<td>Message Tracking Traces</td>
<td>Connection Message Transfer Agent</td>
<td>diag_MTA_*.uc</td>
</tr>
<tr>
<td>(see also “Message delivery and retrieval” in</td>
<td></td>
<td>Connection System Agent</td>
<td>diag_CuSysAgent_*.uc</td>
</tr>
<tr>
<td>Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td></td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Tomcat Application</td>
<td>diag_Tomcat_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection IMAP Server</td>
<td>diag_CuImapSvr_*.uc</td>
</tr>
<tr>
<td>NDRs</td>
<td>Call Flow Diagnostics</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>(see also “NDRs” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notifications not sent</td>
<td>Traces for Other Notification Problems (expand the macro trace to select SIP or SCCP)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td>(see also “Notifications not sent” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td>Message not synchronized in Unified Messaging</td>
<td>Single Inbox Traces</td>
<td>Connection Mailbox Sync</td>
<td>diag_CuMbxSync_*.uc</td>
</tr>
<tr>
<td>MWI Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MWIs</td>
<td>Traces for MWI problems (expand the macro trace to select SIP or SCCP)</td>
<td>Connection Conversation Manager</td>
<td>diag_CuCsMgr_*.uc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Notifier</td>
<td>diag_CuNotifier_*.uc</td>
</tr>
<tr>
<td>Networking Issues</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrasite Networking replication</td>
<td>Digital Networking</td>
<td>Connection Digital Networking Replication Agent</td>
<td>diag_CuReplicator_*.uc</td>
</tr>
<tr>
<td>(see also “Intrasite Networking replication” in Table 1: Cisco Unity Connection Serviceability Micro Traces for Selected Problems)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using Micro or Macro Traces

When you use Cisco Unity Connection Serviceability micro traces or macro traces to troubleshoot problems in 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.

Enabling Micro or Macro Traces and View Trace Logs

<table>
<thead>
<tr>
<th><strong>Procedure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
</tbody>
</table>
Traces in 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 using the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI).

Table 3: Cisco Unified Serviceability Traces for Selected Problems lists the information for Cisco Unified Serviceability traces that you need for troubleshooting selected problems and for viewing the trace logs. (For
Enabling Cisco Unified Serviceability traces decreases system performance. Enable traces only for troubleshooting purposes.

Table 3: Cisco Unified Serviceability Traces for Selected Problems

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>Traces to Set</th>
<th>RTMT Service to Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backing up and restoring</td>
<td>Cisco DRF Local Cisco DRF Master</td>
<td>Cisco DRF Local Cisco DRF Master</td>
</tr>
<tr>
<td>LDAP synchronization</td>
<td>Cisco DirSync</td>
<td>Cisco DirSync</td>
</tr>
<tr>
<td>Web application sign-in</td>
<td>Cisco CCMRealm Web Service</td>
<td>Cisco CallManager Realm</td>
</tr>
</tbody>
</table>

Using 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.

Enabling Cisco Unified Serviceability Traces and View Trace Logs

1. In Cisco Unified Serviceability, on the Trace menu, select Troubleshooting Trace Settings.
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.
3. Reproduce the problem.
5. In RTMT, on the System menu, select Tools > Trace > Trace & Log Central.
6. In the Trace & Log Central tree hierarchy, double-click Collect Files.
7. In the Select CUC Services/Application tab, select Next.
8. In the Select System Services/Applications tab, check the check boxes for the applicable service and select Next.
9. In the Collection Time group box, specify the time range for which you want to collect traces.
10. In the Download File option group box, specify the options you want for downloading traces.
11. Select Finish.
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**.
Grammar Statistics Tool

The Grammar Statistics tool shows information about the dynamic name grammars that are used by the 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 Unity 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 recomplied.

By default, Unity 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 Unity 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 Unity 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 Unity 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

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

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


### Task Management Tool

The Task Management pages list a variety of system maintenance and troubleshooting tasks that 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.

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some tasks are critical to Unity Connection functionality. Disabling or changing the frequency of critical tasks may adversely affect performance or cause Unity Connection to stop functioning.</td>
</tr>
</tbody>
</table>

### Accessing the Task Management Tool

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

Cisco Voice Technology Group Subscription Tool

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

Real-Time Monitoring Tool

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 Unity Connection. RTMT can connect directly to devices via HTTPS to troubleshoot system problems. RTMT can also monitor the voice messaging ports on 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 Unity Connection. When a Unity Connection cluster is configured, you can open multiple instances of RTMT to monitor voice messaging ports on each server in the Unity Connection cluster.


Cisco Unified Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool for 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.

**Remote Database Administration Tools**

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


**Cisco Utilities Database Link for Informix (CUDLI)**

The Cisco Utilities Database Link for Informix (CUDLI) tool allows you to navigate the 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**

The Remote Port Status Monitor (rPSM) provides a real-time view of the activity of each voice messaging port on 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**

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 Unity 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 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 Unity 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 Unity Connection, although they are disabled by default. For more information on audit logging, see the “Configuring the Audit Log” chapter of the applicable Cisco Unified Serviceability Administration Guide at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Network Analyzer

The Network Analyzer is a tool that allows administrators to analyze the state of the network and monitor every node through visual representation of the network topology. It also enables administrators to synchronize the data in HTTP(S) networking through tool itself.

For more information on network analyzer, see the network analyzer documentation available at http://www.ciscounitytools.com/Applications/General/NetworkAnalyzer/Help/ConnectionNetworkAnalyzer.htm.

System Restore Tool

To diagnose the issues related to System Restore Tool, you can view the ERRORS.log file created at path /common/RestorePoints/recent. You can also use the diag_CuSysAgent.uc logs to troubleshoot issues corresponding to System Restore sysagent task. This section further covers the errors that you might get while using System Restore Tool.

Database Error While Creating Restore Point

If you are getting the "Database is not online" error while creating a restore point through CLI, reboot the system to get the database up.

Error in Index Validation

If you are getting any or all of the following errors related to index validation in ERROR.log file, drop and recreate the corrupted indexes.

- ERROR: Bad key information in TBLspace description.
- ERROR: Index ix_tbl_message_messageobjectidtypepriority for unitymbxdb1:informix.tbl_message is bad.
Error in Index Validation
CHAPTER 3

Troubleshooting Cisco Unity Connection Deployments

- Troubleshooting Installation Issues, on page 25
- Troubleshooting Upgrade Issues, on page 26
- Troubleshooting SELinux Issues, on page 26

Troubleshooting Installation Issues

If you receive an error during installation of Cisco Unity Connection, do the following:

- Check if you are meeting the platform requirements mentioned in Cisco Unity Connection 11.x Supported Platforms List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

- Make sure that you have met the software requirements mentioned in System Requirements for Cisco Unity Connection Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

- Check if the problem is because of SELinux mode on publisher server during the installation of a subscriber server. See Troubleshooting SELinux Issues section.

- Review install logs to diagnose the problem. You can use CLI command or RTMT to collect installation logs. For more information on collecting logs from CLI command, see “file get” section of the “File Commands” chapter of the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions. For information on collecting logs from RTMT, see the “Collect Installation Logs” section of the “Traces and Logs” chapter of the applicable Cisco Unified Real-Time Monitoring Tool Administration Guide. You can locate both the guide at http://www.cisco.com/en/us/support/unified-communications/unified-communications-manager-collmgr/products-maintenance-guides-list.html.

  Note

  If you receive any error while installing the subscriber server, you can review the install logs of the subscriber server to troubleshoot the problem.

- Contact Cisco TAC if you are not able to resolve the issue.
Troubleshooting Upgrade Issues

Following are the issues that you might face while upgrading from one version of Unity Connection to another:

- **Switch Version Failures**: To troubleshoot the switch version failures as a part of upgrade from Unity Connection 8.6 to a later version, verify whether the problem is caused by SELinux security policies. For more information, see the Troubleshooting SELinux Issues section. You can also review install logs for upgrade failure. For more information on how to collect install logs, see applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions and Cisco Unified Real-Time Monitoring Tool Administration Guide at http://www.cisco.com/en/us/support/unified-communications/unified-communications-manager-collmgr/products-maintenance-guides-list.html.

  **Note**  
  Make sure to run pre upgrade CLI to verify if the system is good to upgrade.

Troubleshooting Locale Issues After Upgrade

If you face any problem related to locale after upgrade, do the following:

**Step 1** Check if the locale is installed or not using the show cuc locales CLI command.

**Step 2** In Cisco Unity Connection Administration, navigate to Users > Users and select a user for whom locale is not displaying correctly.

**Step 3** Verify that the correct language is selected from the language drop-down list.

**Step 4** Click Save to apply the settings.

Troubleshooting SELinux Issues

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

**Step 2** If SELinux is in Enforcing mode, run the CLI command `utilos secure permissive` to put the Unity Connection server in Permissive mode.

**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 Unity Connection server in Enforcing mode by running the CLI command `utilos secure enforce`.
  c) Try to create the symptom again.
  d) Create the audit logs diagnostic file by running the CLI command `utilos 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 active log syslog/security-diagnostics.tar.gz.
Step 5  Contact Cisco TAC.
Troubleshooting SELinux Issues
CHAPTER 4

Troubleshooting User and Administrator Access

• Unity Connection Not Responding to Key Presses, on page 29
• Users Do Not Hear Sign-in or Desired Prompt When Calling Unity Connection, on page 30
• Administration Accounts Unable to Sign-In to Cisco Unity Connection Serviceability, on page 31
• User Account is Locked over TUI/VUI Interface, on page 31
• User Account is Disabled over Web Applications, on page 31
• Troubleshooting Sign-in Problems with Visual Voicemail (Pin Based Authentication), on page 32
• Troubleshooting Sign-in Problems with Visual Voicemail (Password Based Authentication), on page 32
• ErrorMessageAppearsWhileUpdatingthePhonePINthroughCiscoUnityConnectionAdministration orCiscoPCA, on page 33
• User DisplayNameNotGetUpdatedafterAD Synchronization, on page 33

Unity Connection Not Responding to Key Presses

When Unity Connection is integrated with Cisco Unified Communications Manager using SCCP, Unity Connection may not respond to key presses. In such 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 available in Cisco IOS software version 12.0(5) and later.

In Cisco IOS software-based gateways that use H.245 out-of-band signaling, you need to enable DTMF relay. However, in the Catalyst 6000 T1/PRI and FXS gateways, DTMF relay is enabled by default.

Enabling DTMF Relay

Step 1 On a VoIP dial-peer servicing 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 Unity Connection.

What to do next
Verifying DTMF settings

**Step 1** In Cisco Unity Connection Administration, navigate to Telephony Integrations > Port Group.

**Step 2** On the Search Port Groups page, select the port group of which you want to verify the DTMF settings.

**Step 3** On the Port Group Basics page, navigate to Edit > Advanced Settings.

**Step 4** On the Edit Advanced Settings page, verify that the Use DTMF KPML and Use DTMF RFC 2833 check boxes are checked.

**Users Do Not Hear Sign-in or Desired Prompt When Calling Unity Connection**

When a user calls 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 sends the call to the Attempt Sign-In conversation.

Unity 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, Unity 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 Routing Rules 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 Using Diagnostic Traces for Troubleshooting, on page 1 section.

Unity Connection also provides Port Status Monitor tool that you can use to troubleshoot call routing problems. To use Port Status Monitor tool for troubleshooting issues, do the following:

**Using Port Status Monitor**

**Step 1** Download and install Port Status Monitor from Cisco unity tools [http://ciscounitytools.com](http://ciscounitytools.com).

**Step 2** Enable CDE, Routing Rules, ConvSub, PhaseServer, and PhaseServerToMonitor traces.

**Step 3** In Cisco Unity Connection Administration, navigate to System Settings > Advanced > Conversations.

**Step 4** On the Conversation Configuration page, make sure that the Enable Remote Port Status Monitor Output checkbox is checked and the IP address of the local machine, that is being used to connect to the server, is specified in the IP Addresses Allowed To Connect For Port Status Monitor Output (comma-separated) text box.
Step 5 Analyze the PSM output to diagnose the problem.

Administration Accounts Unable to Sign-In to Cisco Unity Connection Serviceability

If the default application administration account is locked because of password expiration or too many unsuccessful sign in attempts, you can reset the password using the `utils cuc reset password` CLI command to unlock the account.

User Account is Locked over TUI/VUI Interface

**Problem statement:**
When a user hears the "Your account is locked and cannot be opened. For help please contact System Administrator " prompt while accessing the voicemail account through TUI/VUI interface.

**Resolution:**
Do either of the following to resolve the problem:

- Navigate to Edit User Basics > Password Settings page of Cisco Unity Connection Administration and uncheck the Locked by Administrator check box to unlock the user account.
- Navigate to the Edit User Basics page of Cisco Unity Administration and update the Voicemail Application Access to Active to activate the inactive user account.

**Related Diagnostic Traces:**
- If the CiscoSysLog contains the event "EvtSubAccLockedMaxHack", this confirms that the user has exceeded the maximum number of Sign-in attempts and the user account has been locked.
- If the CiscoSysLog contains the event "EvtSubAccountInactive", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

User Account is Disabled over Web Applications

**Problem statement:**
When a user is getting the "Account has been disabled" error message while accessing the Cisco Unity Connection web interfaces, such as Cisco PCA, Cisco Unity Connection Administration, and Web Inbox.

**Resolution:**
To resolve the issue, navigate to the Edit User Basics page of Cisco Unity Administration and update the Voicemail Application Access to Active to activate the inactive user account.

**Related Diagnostic Traces:**
If the audit logs contains "User with alias <user alias> marked inactive since the user has not logged in since last <configured no. of days>", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

Troubleshooting Sign-in Problems with Visual Voicemail (Pin Based Authentication)

Problem statement:
When the user is getting the "Your account is locked. Contact your administrator to unlock your account" error message while logging into Visual Voicemail (VVM).

Resolution:
Do either of the following to resolve the problem:

• Navigate to Edit User Basics > Password Settings page of Cisco Unity Connection Administration and uncheck the Locked by Administrator check box to unlock the user account.

• Navigate to the Edit User Basics page of Cisco Unity Administration and update the Voicemail Application Access to Active to activate the inactive user account.

Related Diagnostic Traces:

• If the audit logs contains "Failed to Login to Cisco Unity Connection VMWS", this confirms that the user has exceeded the maximum number of Sign-in attempts and the user account has been locked.

• If the audit logs contains "User with userName <alias> is inactive due to inactivity timeout", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

Troubleshooting Sign-in Problems with Visual Voicemail (Password Based Authentication)

Problem statement:
When the user is getting the "Please enter a valid username and password pair" error message while logging into Visual Voicemail (VVM) with valid credentials.

Resolution:
Do either of the following to resolve the problem:

• Navigate to Edit User Basics > Password Settings page of Cisco Unity Connection Administration and uncheck the Locked by Administrator check box to unlock the user account.

• Navigate to the Edit User Basics page of Cisco Unity Administration and update the Voicemail Application Access to Active to activate the inactive user account.

Related Diagnostic Traces:
The audit log contains "Failed to Login to VMREST", this confirms that user account has been either locked or disabled due to inactivity timeout.

**Error Message Appears While Updating the Phone PIN through Cisco Unity Connection Administration or Cisco PCA**

If the "Bad response from CUCM. Reason: Requested resource is not available " error message appears while updating the phone PIN through Cisco Unity Connection Administration or Cisco PCA, make sure that:

- The username and password of primary AXL server entered on the Edit AXL Servers page are correct.
- The AXL server is up and running.
- The Ignore Certificate Errors check box is checked. If the check box is not checked, confirm that Unity Connection has successfully validated the certificates for AXL server.

To troubleshoot more problems related to PIN synchronization, see the traces in "Micro Traces for Selected Problems" section of the "Troubleshooting Cisco Unity Connection" chapter.

**User Display Name Not Get Updated after AD Synchronization**

When a user is imported from Active Directory to Unity Connection first time, Display Name of the user is formed with First Name and Last Name. If Administrator changes the First Name and Last Name of the user on Active Directory, then the Display Name of the user may not be updated on Unity Connection automatically after AD synchronization.

In this case, you need to update the Display Name of the users manually either through Edit User Basics page of Cisco Unity Connection Administration or using Bulk Administration Tool (BAT).

To update the Display Name of the users through BAT, do the following:

- On Cisco Unity Connection Administration, navigate **Tools > Bulk Administration Tool**.
- Export all users into CSV file on the Bulk Administration Tool page. The CSV file contains all the user related fields such as Alias, Extension, First Name etc.
- Copy the Alias, First Name and Last Name information of all the users into a new CSV file.
- In CSV file, create a new column for Display Name of the users and fill the column for user's Display Name formed by First Name and Last Name.
- Select **Update** on Bulk Administration Tool page and upload the CSV file for updating the Display Name of all the users.

For more information on Bulk Administration Tool, see "Bulk Administration Tool" chapter of System Administration Guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration-guide/b_cucsag.html
User Display Name Not Get Updated after AD Synchronization
Troubleshooting Call Transfers and Call Forwarding

Calls Not Transferred to the Correct Greeting

When calls are not transferred to the correct greeting, use the following task list to determine the cause and to resolve the problem.

Following are the tasks to troubleshoot call transfers to wrong greetings:

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 Confirm that Forward Timer in the Phone System is in Synch with the Rings to Wait For Setting in Unity Connection.

2. Confirm that the phone system programming enables callers to hear the personal greeting of the user. See the Confirm that Phone System Integration Enables Playing the User Personal Greeting for Callers.

3. Confirm that the busy greeting is supported and enabled. See the Confirming that Busy Greeting is Supported and Enabled.

4. Confirm that the caller reaches the intended destination based on the search scope. See the Confirming that Search Scope Configuration Sends Call to Intended Destination.

5. Make sure that * or the pattern you want to allow is not mentioned in the Default System Transfer or Default transfer restriction tables. To verify this, navigate to System Settings > Restriction Tables and select the restriction table in which you want to verify the settings.

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

Confirm that Forward Timer in the Phone System is in Synch with the Rings to Wait For Setting in 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 Unity Connection waits before taking a message.

If the phone system is forwarding the call to another extension before Unity 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.

Synchronizing 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 > and select Users. On the Search Users page, select the alias of the user whose calls are not being routed to the correct greeting.

**Step 3**
On the Edit User Basics page, on the Edit menu, select Transfer Rules.

**Step 4**
On the Transfer Rules page, select the name of the active transfer rule.

**Step 5**
On the Edit Transfer Rule page, under Transfer Action, confirm that the Extension or URI option is selected for the Transfer Calls To field and that the extension number is correct.

**Step 6**
In the Transfer Type list, confirm that Supervise Transfer is selected.

**Step 7**
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 Unity Connection waits before routing the call to the personal greeting of the user.

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

**Step 8**
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 9**
On the Search User Templates page, select the alias of the user template that you want to change.
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 10**
On the Edit User Template Basics page, on the Edit menu, select **Transfer Rules**.

**Step 11**
On the Transfer Rules page, select the name of the active transfer rule.

**Step 12**
On the Edit Transfer Rule page, under Transfer Action, confirm that the **Extension** option is selected for the Transfer Calls To field.

**Step 13**
In the Transfer Type list, confirm that **Supervise Transfer** is selected.

**Step 14**
In the Rings to Wait For field, enter the same setting that you entered in **Step 7**.

**Step 15**
Select **Save**.

---

**Confirm that 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.

**Verifying the Phone System Integration Settings**

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

**Step 2**

**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 Busy Greeting is Supported and Enabled**

When a call arrives at a busy extension and is forwarded to Unity Connection, phone systems typically send the reason for forwarding (the extension is busy) along with the call.

If Unity 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 Integration Guide for Cisco Unity Connection, at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Confirming that Search Scope Configuration Sends Call to 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. 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 Unity Connection objects and be transferred to a different object than the caller expects to reach.

To make a match by extension, Unity Connection checks the search space that is currently defined as the search scope for the call. Unity 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 Using Diagnostic Traces for Troubleshooting.

Problems with Call Transfers (Cisco Unified Communications Manager Express SCCP Integrations Only)

In 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.

Configuring 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

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 Unity Connection conversation when called by Unity Connection.

Correcting the Rings to Wait For Setting

Step 1  In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, select the alias of the user who is hearing a reorder tone when answering a call from Unity Connection.
Step 2  On the Edit User Basics page, on the Edit menu, select Notification Devices.
Step 3  On the Notification Devices page, select the display name of a notification device.
Step 4  On the Edit Notification Device page, under Phone Settings, set the Rings to Wait field to three or more rings and select Save.
Step 5  On the User menu, select Notification Devices.
Step 6  Repeat Step 3 through Step 5 for each remaining notification device.
Step 7  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 8  On the Search User Templates page, select the alias of the user template that you want to change.
Step 9  On the Edit User Template Basics page, on the Edit menu, select Notification Devices.
Step 10 On the Notification Devices page, select the display name of a notification device.
Step 11 On the Edit Notification Device page, under Phone Settings, set the Rings to Wait field to three or more rings and select Save.
Step 12 On the User menu, select Notification Devices.
Step 13 Repeat Step 10 through Step 12 for each remaining notification device.
Step 14 Expand Call Management, then select System Call Handlers.
Step 15 On the Search Call Handlers page, select the display name of a call handler.
Step 16 On the Edit Call Handler Basics page, on the Edit menu, select Transfer Rules.
Step 17 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 Unity Connection, contact Cisco TAC.

Troubleshooting Directory Handler Searches

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 is selected, 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 Not Found in the Search Scope of Directory Handler.

For voice-enabled directory handlers, the voice-recognition engine does not recognize the names. See the Voice Commands Recognized But Names Not Recognized, on page 174.

Users Not Found in the Search Scope of 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 the Search Space Used During a Call for instructions on using traces to determine the inherited search scope.

Troubleshooting Message Addressing

Message addressing involves the ability to select a desired recipient or recipients when creating a new message. This section covers some problems that the users might experience with message addressing:

- Users Unable to Address 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 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 Unable to Address 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 Returned When a User Addresses by Extension

If a user addresses a message by extension and hears an unexpected match, the most common cause can be the search space configuration. To make a match by extension, Unity Connection checks the search space of the user who is addressing the message. Unity 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 Unity 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 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, Unity Connection returns each match.

Caller is Not Getting Prompt in Expected Language

If a caller is not get prompt in expected language, check the following:
• If the locales are installed on both the servers in case of a cluster.

• If the caller is an outside caller for unity connection, then he will always listen prompts in system default language of that unity connection.

• If the call handler language settings of the caller is set to “Inherit Language from Caller”, then for an internal caller, the prompts are played in the caller set language.

• If the caller is an Unity Connection user and logs in to his/her mailbox, then the caller always listen prompts in caller set language.

Using Traces to Determine the Search Space Used During a Call

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 Using Diagnostic Traces for Troubleshooting, on page 1.
User Hears Full Mailbox Warnings

When users hear a prompt related to a full mailbox, it means that the limit of at least one of the following mailbox quotas, which limit the size of voice mailboxes, has reached:

- **Warning Quota:** If a mailbox has reached the size of the warning quota, the user hears a warning that the mailbox is almost full. To resolve the issue, delete the messages until the mailbox size becomes less than the warning quota.

- **Send Quota:** 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 to reduce the mailbox size.

- **Send/Receive quota:** 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, Unity 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.
**Nondelivery Receipt (NDR) Not Received for Undelivered Message**

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

If the original message is malformed, rather than sending the message to the Undeliverable Messages list, Unity 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 Are Delayed**

Following are the tasks to troubleshoot the possible causes for the apparent delay of messages.

**Step 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" section in the "Using Reports" chapter of the Administration Guide for Cisco Unity Connection Serviceability Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/serv_administration/b_11xcucservag.html

**Step 2**


**Messages Are Not Delivered**

See the following troubleshooting steps for investigating messages that are not being delivered to the intended recipients.

- Confirm that the users who are assigned to the Undeliverable Messages distribution list have been forwarding messages to the intended recipients. See the Undeliverable Messages Not Forwarded to Recipients, on page 46 section.
• Confirm that the user mailbox is not full. See the User Has a Full Mailbox, on page 45
• 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 Unity Connection Entities
Deleted and No Replacements Assigned, on page 46 section.

• Review message aging settings. See the "Message Aging Policies" section in the "Message Storage"
chapter of the System Administration Guide for Cisco Unity Connection Release 11.x, available at

• Verify that the message, which got removed from the mailbox, is not flagged for dispatch delivery. If
the two users belongs to a distribution list that is the recipient of a call handler configured to mark
messages for dispatch delivery, then a message is removed from the mailbox of the user as soon as the
message is accepted by another user of the distribution list. See the "Dispatch Messages" section in the
"Messaging" chapter of the System Administration Guide for Cisco Unity Connection Release 11.x,

• 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 Unity Connection Unable to Relay Messages, on page 46

User Has a Full Mailbox

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

• By default, when an unidentified caller attempts to send a message to a user whose mailbox has exceeded
the send/receive quota, Unity Connection still delivers the message. For such scenarios, you can configure
Unity Connection to indicate the caller that the recipient mailbox is full, and prevent the caller from
recording a message for that recipient. To do this, log in to Cisco Unity Connection Administration,
navigate to the Message Storage > Mailbox Quotas page, and 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, Unity 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, Unity 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. In addition, if the user account for the recipient
is configured to send non-delivery receipts when message delivery fails, Unity 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 Unity Connection user
records a message, but the quota is exceeded in the act of delivering the message, Unity Connection
delivers the message regardless of the quota.

If a user whose voice mailbox has exceeded the send quota logs in to Unity Connection and attempts to send
a message to another user, Unity Connection indicates that the send quota has been exceeded and does not
allow the sender to record the message. If a user calls another user and the call 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 Unity 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 Not 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. Therefore, the users of the Undeliverable Messages distribution list should regularly check and forward 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 Unity Connection Entities Deleted and No Replacements Assigned

When you delete a user who was assigned to review the messages that are sent to any of the following 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

Unity Connection Unable to Relay Messages

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 Unity Connection to send all the 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, Unity Connection does not relay messages to the relay address to avoid possible delivery loops. For example, if Unity Connection needs to relay a message to a proxy address, it is possible that the proxy...
address would resolve back to the same Unity 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. If a Unity Connection server is unable to relay message to the correct address, make sure the smarthost entered on the server is correct and reachable. However, if the problem is still not resolved, review the message relay logs mentioned in Micro Traces for Selected Problems, on page 2 section.

Unable to Play Message Audio in Outlook Web Access

When Unity Connection is configured to relay messages to a Microsoft Exchange server (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.

Unable to Receive Notification Emails for Quota Overflow

If a user is unable to receive notification emails for quota overflow, verify the following:

- Verify that the sender (Unity Connection) is not getting an NDR in the mailbox. If the sender is getting an NDR, check the NDR code and take action accordingly. For more information on NDR codes, refer to the "Troubleshooting Non-Delivery Receipts, on page 79 "chapter of this guide.

- Verify that the corporate email address specified for the user is valid and correctly spelled.

- Verify that the corporate mailbox of the user has some free space.
Unable to Receive Notification Emails for Quota Overflow
Troubleshooting Unified Messaging

Troubleshooting Single Inbox Issues

You may face some issues with single inbox that you can troubleshoot using the information provided in the sections mentioned further.

Mismatch of Date and Time for Messages in Unity Connection and Exchange 2003

Following are the circumstances when the date and time Unity Connection received a message is not synchronized with the date and time on Exchange 2003:

• A user already has voice messages when the administrator configures single inbox for the user. In Unity 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 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. Unity Connection resynchronizes the voice message into Exchange. The date and time on the messages in Unity 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 the connectivity between Unity Connection and Exchange 2003 is interrupted and restored. In Unity 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 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 Unity Connection relays SMTP messages. (If DNS is configured, you can also specify the fully qualified domain name of the smart host.) To verify this, log in to Unity Connection Administration,
navigate to the System Settings > SMTP Configuration > Smart Host page and verify the IP address or hostname of smart host.

If messages are being relayed but not as you expect, check how the message actions are relaying messages for a specific user through the Message Actions page in Unity Connection Administration for that user.

If messages are disappearing, see the Unity Connection Unable to Relay Messages, on page 46.

Single Inbox Not Working for Anyone on Unity Connection

When single inbox is not working for any of the users on a Cisco Unity Connection server (for example, Unity Connection voice messages are not synchronized into Office 365 and the 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 status of the Connection Mailbox Sync (in the Critical Services section) service is Started:

2. If a firewall is configured between the Unity Connection and Exchange servers or between Unity 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” chapter in the Security Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

Single Inbox Not Working for Unified Messaging Users

When single inbox is not working only for the Unity 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 Unity Connection-specific tasks only on the primary (active) server.

1. Confirm that the unified messaging service is enabled and that single inbox is enabled:
   In Unity Connection Administration, expand Unified Messaging and select Unified Messaging Services.
   On the Search Unified Messaging Services page, select the unified messaging service of which you want to check the status.
   On the Edit Unified Messaging Service page, confirm that the Enabled check box is checked.
   Confirm that the Synchronize Unity Connection and Exchange Mailboxes (Single Inbox) check box is checked.

2. Test the unified messaging service:
   In Unity Connection Administration, expand Unified Messaging and select Unified Messaging Services.
   On the Search Unified Messaging Services page, select the unified messaging service that you want to test.
   On the Edit Unified Messaging Service page, select Test.
   Correct any problems that are listed on the Task Execution Results page.

3. Test one of the affected unified messaging accounts:
   In Unity Connection Administration, expand Users and select Users.
   On the Search Users page, select the user for which you want to update the unified messaging account.
   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 or Office 365, but the public certificates from the certification authority (CA) that signed the certificates on the Exchange servers have not been uploaded to the Unity Connection server.

   **404 error:** (Exchange Only) 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 Unity Connection user associated with this unified messaging service:

   In Unity Connection Administration, expand Unified Messaging and select Unified Messaging Services. On the Edit Unified Messaging Service page of the select unified messaging service, in the Username and Password fields, replace the credentials for the unified messaging services account with the credentials for a Unity Connection user associated with the service.

   Send the user a Unity Connection voice message, and determine whether the voice message synchronized to Exchange or 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.

   Switch the Username and Password fields back to the values for the unified messaging services account.


   Send the Unity Connection user another voice message, and determine whether the voice message synchronized to Exchange or 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. 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 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.


9. (Office 365 Only) Confirm that Office 365 servers, which Unity Connection accesses have authentication mode set to Basic.

10. If you configured the unified messaging service to validate certificates for Exchange or Office 365 servers or for Active Directory domain controllers:

    - Confirm that the applicable certification authority certificates have been uploaded to the Unity Connection server.

    - Confirm that the certification authority certificates have not expired.
11. (Exchange Only) If all Unity 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:

   Confirm that certification authority certificates have been uploaded to the Unity Connection server.

   In Unity 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.

   Confirm that the SSL certificates have not expired.

12. (Exchange Only) Use Microsoft EWSEditor to access the Exchange mailbox of a Unity Connection user using the unified messaging services account. This allows you to determine whether the problem occurs even when Unity Connection is not involved.

   EWSEditor software and documentation are available on the Microsoft website.

   1. Confirm DNS settings:

      • Confirm that the Exchange server is reachable from Unity Connection.

      • If you configured the unified messaging service to search for Exchange or Office 365 servers, confirm that the Unity Connection server is configured to use DNS.

      • If you configured the unified messaging service to search for Exchange or Office 365 servers, confirm that the name of the Exchange or Office 365 server is resolvable by the DNS server that Unity Connection is configured to use.

      • If you configured the unified messaging service to search for Exchange or Office 365 servers, confirm that the DNS server that Unity Connection is using is configured with appropriate records for auto-discovery.

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

When single inbox is not working (for example, Unity 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 Unity Connection users but not for all users associated with a unified messaging service, do the following tasks.
When a cluster is configured, do the Unity Connection-specific tasks only on the primary (active) server.

1. In Unity Connection Administration, expand Users and select Users. On the Edit User Basics page, in the Edit menu, select Unified Messaging Accounts. On the 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.

3. In Cisco Unity Connection Administration, expand Users and select Users. On the Edit User Basics page, in the Edit menu, select Unified Messaging Accounts. On the Unified Messaging Accounts page for the user, confirm that single inbox is enabled in one of the user’s unified messaging accounts.

4. In Cisco Unity Connection Administration, expand Users and select Users. On the Edit User Basics page, in the Edit menu, select Unified Messaging Accounts. On the Unified Messaging Accounts page for the user, confirm that Unity Connection is configured to use the correct Exchange email address.

5. In Cisco Unity Connection Administration, expand Users and select Users. On the Edit User Basics page, in the Edit menu, select SMTP Proxy Addresses. On the 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.

Note

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 Unity Connection to search for Exchange servers, determine whether Unity Connection is able to automatically detect mailbox moves. See the “Configuring Unified Messaging” chapter in the Unified Messaging Guide for Cisco Unity Connection Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

1. 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 “Configuring Unified Messaging” chapter in the Unified Messaging Guide for Cisco Unity Connection Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

2. If single inbox is not working for all of the Unity 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, Unity Connection 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.

3. If single inbox is not working for all of the Unity 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 Unity 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 Unity Connection server.
• Confirm that the SSL certificates have not expired.

**Single Inbox Synchronization from Exchange is Delayed**

If Unity 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 Unity 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 Unity 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 Unity Connection server (confirm that port 7080 is open in the firewall, if applicable):

   ```bash
telnet <IP address of the Unity Connection server> 7080
   ```

   If no error message is returned, the Exchange server was able to connect to the Unity Connection server. If an error message is returned:
   • In Cisco Unity Connection Serviceability, confirm that the Unity Connection Jetty service is **running**.
   • Troubleshoot the network problem.

   Press **Ctrl-K** to exit from Telnet.

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

   If you Reset a particular unified messaging service, the synchronization is delayed for all of the users associated with the unified messaging service as Unity Connection resynchronizes data with Exchange.

   If the synchronization from Exchange is delayed, you can also check if the number of outstanding requests is consistently not exceeding 999. To check the number of outstanding request, you need to enable the CsMbxSync (level 19) traces. For more information on traces, see **Traces in Cisco Unity Connection Serviceability**, on page 1.

   If the number of outstanding requests is consistently increasing to a value greater than 999, check the EWS latency (EWS request-response RTT time) between Unity Connection and Exchange Server. If the latency is more than the supported value, calculate the number of connections and change the number of connections to a calculated value. For information on maximum EWS latency and the method to calculate connections, see the “Calculating the Number of Connections for One Unity Connection Server” section of the Single Inbox in Cisco Unity Connection 11.x chapter of Design Guide for Cisco Unity Connection Release 11.x [https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/design/guide/b_11xcucdg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/design/guide/b_11xcucdg.html).

**Single Inbox Synchronization from Office 365 is Delayed**

If Unity 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 Unity 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**.

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

### Single Inbox Synchronization from Exchange Failed

If synchronization from Unity 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 Fails with Office 365 Using ADFS

If you are integrating 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, the Single Inbox may not work as Unity Connection is not equipped to handle ADFS.

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

### Duplicate Message Issue with Single Inbox

*Internet Message ID* is a unique identifier for internet messages. Cisco Unity Connection assigns a unique Internet message ID to each voice message. If messages are restored with same internet message ID, the duplicate messages are created in the mailbox of a user. When mailbox synchronizes with Exchange, the duplicate messages are reflected in the Single Inbox.

To resolve the issue of duplicate messages in Single Inbox, a user or administrator must delete the duplicate messages from the mailbox.

---

**Note**

COBRA is one of the interfaces that provide the option to restore the messages as duplicate messages. To avoid the duplicate message issue in Single Inbox, do not select the option to restore the messages as duplicate messages.
Resolving 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 and select Save. (Enter the fully qualified domain name of the server only if DNS is configured.)

Step 3
In Cisco Unity Connection Administration, expand System Settings and select General Configuration.

Step 4
On the General Configuration page, in the When a recipient cannot be found list, select Relay message to smart host.

Step 5
Click Save.

Step 6
In Cisco Unity Connection Administration, expand Users > Message Actions and select the Accept the message option from the Voicemail drop-down list.

Step 7
Enter an SMTP Proxy Address for the relay address field.

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
Setup a recipient policy on Exchange Server such that the Unity Connection alias resolves to the corporate email Id.
- For Exchange 2013 or Exchange 2010, see the following link:
- For Exchange 2007, see the following link: http://technet.microsoft.com/en-us/library/bb232171(v=exchg.80).aspx
- For Exchange 2003, see the following link:
  http://support.microsoft.com/kb/822447
- For Configuring Exchange Email Policies with Unity Connection, please see the following white paper link:

Troubleshooting Problems with Cisco ViewMail for Microsoft Outlook

You may face some issues with ViewMail for Outlook that you can troubleshoot using the information provided in the sections mentioned further.

Voice Messages or Receipts are Not Received in the Outlook Inbox

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 Unity Connection mailbox quotas configured, and if a user has exceeded the send/receive quota, Unity Connection prevents messages from being received in the user’s Unity 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 Unity 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

If single inbox users cannot send messages through the 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 Unity Connection.

• The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found, Unity 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 Unity Connection Administration. By default, Unity Connection sends an NDR.

Messages Received in an Email Account Other than the Single Inbox Account

If users unexpectedly receive voice messages in their corporate or other email accounts rather than their 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 Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found and Unity 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” section of the “User Settings” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration-guide/b_cucsag.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 Unity Connection Administration, see the Message Actions page for that user.

Messages cannot be Played in Outlook

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

Messages Moved into a .PST Folder in Outlook cannot be Played

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

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

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

When Unity Connection replicates a secure voice message to Exchange, the replicated message contains only text that briefly explains secure messages; only the copy of the .wav file remains on the Unity Connection server. When a user plays a secure message using ViewMail for Outlook, ViewMail retrieves the message from the Unity 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 Unity Connection Inbox folder, the only copy of the voice message is moved to the deleted items folder in Unity 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 Unity Connection Inbox folder, and:

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


Playing a Message Does Not Turn Off the Message Waiting Indicator

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

- Two copies of migrated messages 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 remains unread in Unity Connection, and the message waiting indicator remains 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 turns off the message waiting indicator as appropriate.
Message Waiting Indicator Turns Off Before the Message is Played

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

Deleting a Message in Outlook Does Not Delete the Corresponding Message

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

- Two copies of migrated messages 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 remains in the user’s inbox in Unity Connection. Deleting the migrated message in Outlook (the copy that was synchronized into the Exchange mailbox by the single inbox feature) causes the message to be moved from the user’s inbox in Unity Connection to the user’s deleted items folder in Unity Connection.

Messages Moved into a .PST Folder in Outlook are Deleted

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


Troubleshooting Problems with Invalid Passwords

When users change their Cisco Personal Communications Assistant (PCA) password in the Messaging Assistant, they must also update the password configured in ViewMail options so that the client can continue to access Unity 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.
Changing 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**.

**Step 2** 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 3** From the Associated Email Account list, select the Microsoft Exchange/Single Inbox account for the user and select **Edit**.

**Step 4** On the Viewmail Account Settings window, change the password for the user.

**Step 5** Select **Test Settings**.

**Step 6** If the test passes successfully, select **OK**. If the test fails, reenter the password and repeat.

**Step 7** 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.

Enabling 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**.

**Step 2** 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 3** Check the **Turn on Diagnostic Traces** check box.

**Step 4** Select **OK**.

**Step 5** Reproduce the problem.

**Step 6** 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.

**Step 7** 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 Unity Connection Server for Problems with Single Inbox and ViewMail for Outlook

You can enable the Unity Connection VMO macro trace to troubleshoot client problems from the server side. For detailed instructions on enabling and collecting diagnostic traces, see the Using Diagnostic Traces for Troubleshooting, on page 1.

Troubleshooting Access to Emails in an External Message Store

User on the Phone Hears “Invalid Selection” after Pressing Seven

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

Enabling User Access to Email in an External Message Store

| Step 1 | In Cisco Unity Connection Administration, expand Users and select Users. On the Search Users page, select an applicable user. |
| Step 3 | On the Unified Messaging Accounts page, select the name of the unified messaging service that connects to the external message store. |
| Step 4 | On the Edit Unified Messaging Account page, check the Access Exchange by Using Text to Speech (TTS) check box and select Save. |

User on the Phone Hears “Your Messages are Not Available” after Pressing Seven

When a user has signed in by phone, presses seven 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.

Follow the given steps for troubleshooting a “Your Messages are Not Available” after pressing seven:

1. Test the unified messaging service that enables access to email in the external message store, and correct any errors that are reported. See the Testing the Unified Messaging Service to Access Emails in an External Message Store.

2. Test the unified messaging 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 Unified Messaging Account for User to Access Email in an External Message Store.

3. In Cisco Unity Connection Administration, expand Class of Service and select Class of Service. Select the class of service applied to voicemail users. On the Edit Class of Service page, confirm that the Allow Access to Exchange Email by Using Text to Speech (TTS) check box is checked.

4. In Cisco Unity Connection Administration, expand Users and select Users. Confirm that the Allow Access to Exchange Email by Using Text to Speech (TTS) check box is checked. See the Enabling User Access to Email in an External Message Store.
5. Ping the server to which the unified messaging service connects using the value in the Server field on the Unified Messaging> Unified Messaging Services> if you select Specify an Exchange Server check box, enter the IP address or hostname of the Exchange 2003 server. If the ping fails, Unity Connection is not functional. You must restore the net work functionality to Unity Connection.

6. If the unified messaging service is configured for SSL and the Validate Certificates for Exchange Servers check box is checked, determine whether certificate validation is causing the problem. In Cisco Unity Connection Administration, go to Unified Messaging> Unified Messaging Services and uncheck the Validate Certificates for Exchange Servers check box and select Save.

7. (Exchange 2003 only) Follow the given steps for Exchange 2003 only:

   In Unity Connection Administration, on the Users > Edit Unified Messaging 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 Unity Connection Alias, the user Exchange login alias must match the Unity Connection user alias.

   On the Exchange server, confirm that the Microsoft Exchange IMAP4 service is running.

   Confirm that the Exchange server is set up to support basic authentication for IMAP4.

---

**Testing the Unified Messaging Service to Access Emails in an External Message Store**

**Step 1**  
In Cisco Unity Connection Administration, expand **Unified Messaging** and select **Unified Messaging Services**. On the Search Unified Messaging Services page, select the name of the applicable service.

**Step 2**  
On the Edit Unified Messaging Service page, select **Test**.

**Step 3**  
In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

**Step 4**  
Repeat Step 2 and Step 3 until the test succeeds.

---

**Testing Unified Messaging Account for User to Access Email in an External Message Store**

**Step 1**  
In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select the alias of the user.

**Step 2**  
On the Edit User Basics page, in the Edit menu, select **Unified Messaging Accounts**.

**Step 3**  
On the Unified Messaging Accounts page, select the name of the applicable unified messaging account and 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 2 and Step 4 until the test succeeds.

---

**Enabling User Access to Email in an External Message Store**

**Step 1**  
In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select the alias of the user.

**Step 2**  
On the Edit User Basics page, in the Edit menu, select **Unified Messaging Accounts**.
Step 3  On the Unified Messaging Account page, select the name of the unified messaging service that connects to the external message store.

Step 4  On the Edit Unified Messaging Account page, check the Access Exchange Email by Using Text to Speech (TTS) check box and select Save.

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 (Exchange 2003 Only)

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.

Unity Connection uses the IMAP protocol to interact with Exchange 2003. Exchange 2003 handles messages that are soft-deleted via IMAP differently than those that are soft-deleted 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.

Using Traces to Troubleshoot Access to Emails in an External Message Store

You can use traces to troubleshoot access to emails in an external message store. For detailed instructions, see the Using Diagnostic Traces for Troubleshooting, on page 1.

Troubleshooting Calendar Integrations

Using 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.

Testing the Calendar Integration

**Step 1**
In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, select the alias of a user.

**Step 2**
On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

**Step 3**
On the Unified Messaging Accounts page, select the name of the applicable unified messaging service account.

**Step 4**
On the Edit Unified Messaging Account page, select **Test**.

**Step 5**
In the Task Execution Results window, refer to the list of issues and recommendations and do the applicable troubleshooting steps.

**Step 6**
Repeat **Step 4** and **Step 5** 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 Unity Connection configuration status.

Test Fails the Last Check

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:

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”.

Troubleshooting Guide for Cisco Unity Connection Release 11.x
• 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. (Exchange 2003 only) In Cisco Unified Operating System Administration, on the Services > Ping Configuration page, confirm that Unity 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.

In 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, uncheck the Validate Server Certificate check box and select Save.

On a phone, sign in as the user who experiences the problem and access calendar information.

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 Unity Connection as a trusted certificate, that it is self-signed, and that it has not expired.

In Unity 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 Unity Connection times out, in Unity 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 Calendar 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. 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. Unity 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 Unity Connection times out, in Unity 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.

2. Confirm that the system clocks on the Unity Connection and Exchange servers are both correct.

3. 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 Unity Connection uses to access calendar information is not correctly configured.

Configuring the Unity 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 Unity 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.
Changing 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 Unity 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 Unity 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 Unity 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.

In the Calendars: Short Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Unity 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 3**
Select Save.

"Access Exchange Calendar and Contacts" Option 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:

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 Diagnostic Traces for Troubleshooting, on page 1.

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

You can use traces to troubleshoot issues related to accessing calendar information when using personal call transfer rules. For detailed instructions, see the Using Diagnostic Traces for Troubleshooting, on page 1.

• See also the Troubleshooting Personal Call Transfer Rules, on page 203 chapter.
Changing the Interval Unity Connection Waits to Update Calendar Information

SUMMARY STEPS

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

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 Unity Connection waits between polling cycles when it caches upcoming Outlook calendar data for users who are configured for a calendar integration.

3. Select **Save**.

DETAILED STEPS

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

In the Calendars: Short Calendar Caching Poll Interval (In Minutes) field, enter the length of time that Unity 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 3**
Select **Save**.

Troubleshooting the Test Button for Unified Messaging Services and Unified Messaging Accounts

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

- Unified Messaging > Unified Messaging Services> select a unified messaging service on the Search Unified Messaging Services page> Edit Unified Messaging Services page.
- Users > Users > select a user on the Search Users page> Edit User Basics page> Edit> Unified Messaging Accounts> select an applicable account> Edit Unified Messaging Account page.

For information on using traces to troubleshoot problems with the Test button, see the Using Diagnostic Traces for Troubleshooting, on page 1.
Troubleshooting IMAP Clients and ViewMail for Outlook

Troubleshooting IMAP Clients and ViewMail for Outlook

Troubleshooting Problems with Changing Passwords

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 Unity 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 (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 Unity Connection user account may have been locked by an administrator.
  - The Unity Connection user password may have expired.
• The Unity Connection user account may have been configured to require that the user specify a new password.
• The Unity 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; 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 Unity Connection and Outlook prompts for the username and password.

Troubleshooting Sign-In Problems with IMAP Email Clients (When LDAP is Configured)

If you are using LDAP authentication and using an IMAP email client to access Unity Connection voice messages, and if users who are integrated 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 Unity 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 Unity Connection, restart the Unity Connection IMAPServerservice in Cisco Unity Connection Serviceability. If other web applications are accessing Unity 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 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 Unity 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 Unity Connection IMAPServerservice in Cisco Unity Connection Serviceability, and try again.
Troubleshooting Sign-In Problems with IMAP Clients

If users have trouble signing into an IMAP client and recursively receive the pop-up to enter username and password, it indicates that the account has been locked, inactive, or the limit for the maximum concurrent session has reached. To troubleshoot the issue, verify if:

- User is trying to access the IMAP account with invalid credentials. This is confirmed by the presence of "authFail" instance in CiscoSysLog.
  
  To resolve the issue, navigate to Edit User Basics > Change Password (Web Application) page of Cisco Unity Connection Administration and reset the password for the user.

- User is trying to access inactive IMAP account. This is confirmed by the presence of "EvtSubAccountInactive" event is CiscoSysLog.

  To resolve the issue, navigate to Edit User Basic page of Cisco Unity Connection Administration and update the User Status to Active.

- The limit for maximum concurrent IMAP sessions has reached. This is confirmed by the presence of EvtIMAPLogonSessionLimitExceeded of CiscoSysLog. To resolve the issue, see the Unable to Login to IMAP Client section.

Unable to Login to IMAP Client

If the users have trouble signing into an IMAP client and recursively receive the pop-up to enter username and password, it can be because the limit for the maximum concurrent session has reached. This is confirmed by the presence of EvtIMAPLogonSessionLimitExceeded of CiscoSysLog. To resolve the issue, do the following:

1. Fetch the Alias of the user experiencing the problem from CiscoSysLog.

2. Run the following command to fetch the current value of imapsessioncount for the user:

   ```
   run cuc dbquery unitydirdb select * from vw_subscribertimelastcall where subscriberobjectid = (select objectid from vw_subscriber where alias = '<Alias>')
   ```

   where imapsessioncount is the number of IMAP sessions currently open for the user.

3. Ask the user to hang up one of the IMAP sessions if the value of imapsessioncount matches the configured maximum limit for concurrent IMAP sessions.

   For multiple users, if the value of imapsessioncount is within the configured maximum limit or is not decrementing even after reducing the number of open IMAP sessions, disable the feature for immediate solution or contact Cisco TAC. For information on disabling the feature, see "Restricting the Maximum Concurrent Sessions "section of Security Guide for Cisco Unity Connection Release 11.x at [https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsexc.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsexc.html)

Messages Sent from an IMAP Client Not Received

If users cannot send messages through the 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 Unity 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 Unity Connection. See the Checking the IP Address Access List.

• If Unity 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 Unity Connection server.

• The email address of the message sender must exactly match a primary or proxy SMTP address configured in Unity Connection, as follows:
  
  • If the message is being sent from an IMAP client that is authenticated with the Unity 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 Unity Connection server, the email address can match a primary or proxy address that is configured for any user on the Unity Connection server.

• The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found, Unity 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, Unity 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 Unity 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 Unity 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 Unity Connection user or contact.) For detailed instructions on enabling the traces and viewing the trace logs, see the Using Diagnostic Traces for Troubleshooting, on page 1.

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 Unity 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 Unity Connection was refused.

**Checking the Cisco Unity Connection IP Address Access List**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Administration, expand <strong>System Settings</strong> &gt; <strong>SMTP Configuration</strong>, then select <strong>Server</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the SMTP Configuration Page, on the Edit menu, select <strong>Search IP Address Access List</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Confirm that the IP address in use by the IMAP client appears as an entry in the list, and that the Allow Unity Connection check box is checked.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To add a new IP address to the list, select <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the New Access IP Address page, enter an IP address or you can enter a single * (asterisk) to match all possible IP addresses and select <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>On the IP Address page, check the <strong>Allow Connection</strong> 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.</td>
</tr>
<tr>
<td>Step 7</td>
<td>If you have made any changes on the IP Address page, select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**Messages are Received in an Email Account Instead of a Voice Mailbox**

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 Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found and Unity 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” section in the User Settings” appendix of the System Administration Guide for Cisco Unity Connection Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/troubleshooting/guide/b_11xcuctsg.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 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 ViewMail for Outlook

In cases where user email profiles have an Exchange account and the users are using ViewMail for Outlook, 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 Unity 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 Unity Connection user, the message is delivered to the Exchange mailbox of the recipient instead of to the Unity 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 Not Appearing in ViewMail Account Settings in ViewMail for 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.

Unable to Play Messages through ViewMail for 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 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 ViewMail for 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.

ViewMail for Outlook Form Does Not Appear

If the ViewMail for Outlook 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.

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.

Enabling 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 the ViewMail tab.
Step 2 Select Settings.
Step 3 In the Cisco ViewMail Settings > dialog box, check the > Turn on diagnostic traces check box and select OK.
Step 4 Reproduce the problem.
Step 5 Review the resulting log files by selecting the Email Log Files option on the ViewMail tab and sending the resulting message with logs attached to an email address.

Collecting Diagnostics from ViewMail for Outlook on the User Workstation

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

Enabling 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

1. 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
1. Select OK.
2. Reproduce the problem.
3. 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 Unity Connection for IMAP Client Problems

You can use Unity Connection traces to troubleshoot IMAP client problems from the server side. You need to enable the following micro traces to troubleshoot IMAP client problems:

- SMTP (all levels)
- MTA (all levels)
- CulmapSvr (all levels)
- CsMalUmss (all levels)
- CML (all levels)

For detailed instructions on enabling and collecting diagnostic traces, see the Using Diagnostic Traces for Troubleshooting, on page 1 section.

Login via IMAP Fails for LDAPS if IP Address of LDAP Server 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 are 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 cannot connect. The fix for this is for the customer to use DNS if possible.
Troubleshooting Non-Delivery Receipts

Overview

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.

Non-Delivery 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 Unity Connection have the following meanings:

• 4.0.0—An unknown error (for example, connectivity problems) prevented Unity 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 Unity 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 Unity Connection cannot process the message.
• 5.4.4—There are errors in the VPIM configuration in Unity Connection.
• 5.5.4—There was a permanent error in connecting to the SMTP server.
• 5.6.5—The conversion of a Unity 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.
Troubleshooting Transcription (SpeechView)

Task List for Troubleshooting SpeechView

To troubleshoot issues related to SpeechView, do the tasks mentioned in the sub-sections.


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 alerts 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, on page 171 chapter.
   - On the Unified Messaging > SpeechView Transcription > Service page. Make sure that on the Transcription Service for SpeechView page, the Enabled check box is checked.

Many of the warning and error messages on these pages also include information on how to resolve the problem.

1. Confirm that the voicemail users for which SpeechView needs to be enabled have the class of service setting enabled. In Cisco Unity Connection Administration, expand Class of Service and select Class of Service. Select the applicable class of service. On the Edit Class of Service page, check the Allow Users to Access SpeechView Transcription Service check box and select Save.
Issues with a Proxy Server

If accessing the transcription service via a proxy server, troubleshoot the proxy server:


2. Verify that the server designated as a proxy system is configured to advertise transcription services.

3. Continue with this task list on the proxy server.

Issues with the Transcription Service Configuration

1. If the transcription service registration is failing or times out, review the registration task execution results window for specific error messages.

2. If registration has succeeded, use the Test button to troubleshoot the transcription service configuration:

   In Cisco Unity Connection Administration, expand Unified Messaging > SpeechView Transcription and select Services.

   Select the Test button.

   View the test task execution results for specific warnings and error messages.

3. If the test you ran above fails and the transcription service was previously working successfully but has suddenly stopped working, use the Register button to reestablish the registration with the external transcription service:

   In Cisco Unity Connection Administration, expand Unified Messaging > SpeechView Transcription and select Services.

   Select the Register button. Another window displaying the results open. The registration process normally takes several minutes.

   View the registration task execution results for specific warnings and error messages.

4. In Unity Connection Serviceability, verify that the Unity Connection SpeechView Processor and the Unity Connection SMTP Server services are running. See the Confiming that Connection SpeechView Processor and Connection SMTP Server Services are Running.

5. Run the SMTP test to verify that messages can successfully be sent from Unity Connection to an external email account outside of your organization. This SMTP test helps you determine whether the registration problem is due to issues in the communication path to the third-party transcription service. See the Running SMTP Test to Verify Outgoing and Incoming SMTP Path.

Issues Related to User Expectations

1. 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.

1. 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 is not 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.

2. 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 Unity Connection to listen to the message. See the Messages that Cannot be Transcribed for details.

Issues with Transcription Notifications

Troubleshoot the notification device configuration. See the Troubleshooting Notification Devices, on page 153.

Enabling Traces and Contacting Cisco TAC

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.

Confirming that 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 Unity Connection cluster server pair.

The Connection SMTP Server service needs to be running on both servers in a Unity Connection cluster server pair.

Step 1

In Cisco Unity Connection Serviceability, on the Tools menu, select Service Management.
Running SMTP Test to Verify 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 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.

Step 1
On the 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”.


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:

b) Verify that Unity Connection can reach the smart host using the CLI command utilsnetworkping <smarthost>.
c) Verify that the smart host is configured to route messages from the Unity 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 Cisco Unity Connection Administration is being routed correctly. It must be routed by your email infrastructure to the “sti-service” account on the Unity Connection server domain.
For example, 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 Unity Connection SMTP Server component log files to see if the message reached Unity Connection. The SMTP logs are located in diag_SMTP_*.uc. If you see “untrusted client Unity Connection refused” messages in the log files, you need to configure Unity Connection to trust incoming traffic from your email system.


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.

Troubleshooting Transcription Notifications

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.

Step 1 Confirm that messages are being transcribed by following Step 1 through Step 3 in the Task List for Troubleshooting SpeechView.

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, on page 153 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.

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 returns a transcription that instructs the user to call Unity Connection to listen to the message.
Transcription Not Synchronized on User Phones

If a user does not receive transcription on the mobile device not qualified with Unity Connection, make sure that the Hold till transcription received option is enabled for the user. To enable the Hold till transcription received option, navigate to Cisco Personal Communications Assistant > Message Assistant > Personal Options.

However, if the Hold till transcription received option is enabled for a Single Inbox (SIB) user with the SpeechView transcription service, the synchronization of a new voice message between Unity Connection and Exchange mailboxes will be done only when Unity Connection receives the transcription of the voice message from the third-party external service.

Using Diagnostic Traces to Troubleshoot SpeechView

You can use 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 Using Diagnostic Traces for Troubleshooting, on page 1 section.
Troubleshooting Networking

Troubleshooting Intersite Networking Setup

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 Unity 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 Unity Connection Site Gateway

When you create an intersite link in Cisco Unity Connection Administration using the Link to Cisco Unity Site or 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 using DNS.

If DNS is not configured on the 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 does not begin until communication can be established without errors. Do you wish to continue?” (The use of DNS name resolution is optional with Unity 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 Unity Connection encounters this error condition.

Manually Creating 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 Network 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:
   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 Unity Connection Site Gateway

When you create an intersite link in Cisco Unity Connection Administration using the Link to Cisco Unity Site or 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.

**Manually Creating 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 Errors 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 Unity Connection Site Gateway

When you create an intersite link in Cisco Unity Connection Administration, the Unity Connection site gateway checks to see if the combined number of users and contacts on the gateway would exceed the actual limit after the link is created. 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 Unity 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.


"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 Unity Connection 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 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 Unity 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 HTTPS Networking Setup

Unable to Link to Network Location. Cause: Location is Already Part of the network.” Error When Creating an HTTPS Link on Unity Connection”

The error “Unable to link to network location.

Cause: Location is already part of the network” is displayed when you attempt to create an HTTPS link in Cisco Unity Connection Administration under any of the following conditions:

- You attempt to create an HTTPS link from a location to the location itself.
- You attempt to create an HTTPS link from one location L1 to another location L2, and L1 and L2 are already linked to each other in HTTPS network.
• You attempt to create a HTTPS link from a location L1 to another location L2, and L2 already exists in the subtree of the L1.

If you see this error, check the hostname information that you are using to create the link. Verify that you are linking to the correct location and then retry the linking process.

Unable to Link to Network Location. Cause: Publisher (IP Address/FQDN/Hostname) Entered does not Match that on Remote Location Certificate

When you create a HTTPS link from Cisco Unity Connection, and, if you check the Use Secure Sockets Layer (SSL) check box, it verifies whether the entered IPAddress/FQDN/Hostname matches that on the remote location web SSL certificate (the certificate for browsing to the machine over HTTPS). If the values do not match, Cisco Unity Connection Administration displays the error, “Hostname entered does not match that on the remote site certificate.”

When you see this error, you must enter the correct IP/FQDN/Hostname which must matches that on the remote location web SSL certificate or you can use the following procedure and repeat the link creation process to circumvent the error by checking the Ignore Certificate Errors check box.

Creating The HTTPS Link When the Remote Site Gateway Hostname Does Not Match the Name on the Certificate

You can also view the default traces for the Connection Tomcat Application service (trace log filenames matching the pattern diag_Tomcat_*.uc) for further debugging.

Step 1 On the New HTTPS Link page, select Add.
Step 2 For Transfer Protocol, check the Ignore Certificate Errors check box.
Step 3 Configure other settings on the page as applicable, and select Link.

Troubleshooting Directory Synchronization between Two Unity Connections in HTTPS networking

Replication between HTTPS links is accomplished by means of a Feeder service and a Reader service (also referred to as the FeedReader) running on each location. The Reader service periodically polls the remote Feeder service 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 location in order to encrypt the directory information.

The synchronization that occurs within a HTTPS link joined recently can take anywhere from a few minutes to a few hours depending on the directory size. Later updates are only synchronize changes since the last cycle, unless you manually request a full resynchronization.

On a Unity Connection location, 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 Local Network task or the Synchronize Voice Names With Local Network task.

Table 11-1 lists some of the tools you can use to collect information about the operation of the Feeder and Reader applications for HTTPS networking.
Troubleshooting Tools for HTTPS Network

<table>
<thead>
<tr>
<th>Application</th>
<th>Troubleshooting Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader</td>
<td>The Networking &gt; Links &gt; HTTPS Links page displays statistics about the number of HTTPS links and their display names. Each link displays 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 Using Diagnostic Traces for Troubleshooting, on page 1 section for instructions.</td>
</tr>
<tr>
<td>Feeder</td>
<td>• Enable Feeder micro trace levels 00, 01, 02, and 03. See the Using Diagnostic Traces for Troubleshooting, on page 1 section for instructions.</td>
</tr>
</tbody>
</table>

If you want to manually start an incremental update of the directory on either location, you can do so using the Sync button on the Networking > Links > HTTPS Links in Cisco Unity Connection Administration. To initiate a full resynchronization of the entire directory, use the Resync All button on the same page.

You can also collect Cisco Syslogs for RTMT, which help in analyzing the alerts for HTTP(s) Networking. The path to access Cisco Syslogs is /var/log/active/syslog/CiscoSyslog.

Troubleshooting HTTPS Networking Cases

**Distribution Lists and the Members of the Distribution Lists Not Replicating in HTTPS network**

When you create a HTTPS link from Cisco Unity Connection Administration, by default the distribution list and its membership is not synced across the HTTPS network. If you want to enable the synchronization of distribution list and its membership info, enable the "Include distribution lists and membership when synchronizing directory data" check box on the edit page of HTTPS Link.

---

**Note**

If this settings is enabled on one location, then it is required to enable this settings on all the locations which are in HTTPS Network.

When you enable system distribution list synchronization, you cannot disable it after the link is created except by removing and recreating the HTTPS link.

**How to Synchronization Selective Objects from HTTPS link**

There are instances when remote objects could not get synced from a linked HTTPS location and administrator wants to synchronize some specific objects which are reported in the Networking Sync Error Report. There
is a CLI available on command prompt "utilscucnetworkingsynchttps link" which can be used to synchronize these selective objects.


Syntax: utilscucnetworkingsynchttps link [usns | objecttypes] link_display_name usns_list [object_types]

Usage 1: utilscucnetworkingsynchttps link usns link_display_name usns_list

Usage 2: utilscucnetworkingsynchttps link objecttypes link_displayname [object_types]

Parameter Description:

[usns] - option - allows to sync specified USN(s) from the given remote link. Both the parameters link_display_name and usns_list are mandatory.

[objecttypes] - option - allows to sync specified object type(s). Parameter link_displayname is mandatory and object_type is optional.

link_display_name - mandatory parameter - display name of the https link.

usns_list - mandatory parameter to sync USN(s). Maximum of 10 USNs can be specified at once separated by comma (,).

[object_types] - optional parameter for [objecttypes] sync. If no object type is specified then CLI sync all the object types from the specified network link. To synchronization a particular ObjectType such as list or User provide object type with comma (,) separated.

The valid object types are:

1. user
2. list
3. partition
4. searchspace
5. listmember
6. contact.

Note

If link_display_name contains white space(s), it should be included in double quotes.

Example 1:

To synchronize a list of USN's from a https network link.

This example shows the selective synchronization of usn number:167, 171 from https-link-1.

Steps to perform the Selective synchronization

Get the list of USN's values from the USN column of the generated report.

Get the “link_display_name” from HTTP (Link) column of the generated report.

1. Run the following CLI command

   admin:utils cuc networking synchttps link usns https-link-1 167, 171

Example 2:

   Synchronize a particular object type from a HTTPS network link.

   This example shows the selective synchronization of user object type from link https-link-1.

   Steps to perform the Selective sync


   Get the objectType from ObjectType column of the generated report.

   Get the "link_display_name" from HTTP(Link) column of the generated report.

   Run the following CLI command

   admin: utils cuc networking synchttps link objecttypes https-link-1 user

How to Synchronize Selective Objects, Voice Names of a Specific Location in HTTPS Networking

There are instances when remote objects could not get synced from a linked HTTPS node of a particular location and admin wants to synchronize some specific objects which are reported in the Networking Sync Error Report. There is a CLI available on command prompt "utils cuc networking synchttps location" which can be used to synchronize these selective objects.


Syntax: utils cuc networking synchttps location [objecttypes | voicename] location_displayname object_alias

Usage 1: utils cuc networking synchttps location objecttypes location_displayname [object_types]

Usage 2: utils cuc networking synchttps location voicenamelocation_displayname object_alias

[objecttypes] - option : allows to sync specified object type(s) for a particular location in http(s) network. Parameter location_displayname is mandatory and object_types is optional.

[voicename] - option : allows to sync voicename of a particular object using its alias. Both location_displayname and object_alias are mandatory parameters.

location_displayname - mandatory parameter : display name of location joined in http(s) networking.

object_alias - mandatory parameter to sync voice name : Alias of particular object (user/distribution list/contact) whose voicenname needs to be synced.


The valid object types are: a) user b) list c) partition d) searchspace e) listmember f) contact.
Performing the Selective Synchronization for Voicename

Step 1
Identify the home-location of the user u1.
Search for the user u1 on location https-locatio-l1, and fetch the home location of the user u1. For reference let's name it as home-location.abc.com.

Step 2
Use the following CLI command on command prompt to fetch the voice name.
admin: utils cuc networking synchttps location voicename home-location.abc.com u1.

How to Swap Extensions in HTTPS Networking

When you create an HTTPS link from Cisco Unity Connection Administration, the users are synchronized across the HTTPS network. There are instances when user extensions are inter changed at one node and administrator wants to synchronize the extensions across HTTPS remote nodes.

Use case 1:
2. Perform sync across HTTPS network.
3. Change the extension of UserA to 1002 and UserB with Extension 1000 on local node.
4. Change the extension of User A to 1001.
5. After performing steps 3 and 4, the extension of UserA and UserB are inter changed.

6. Again, perform sync across HTTPS network.

When the HTTPS sync is performed and UserA try to update the extension to 1001, which is already assigned to UserB on remote node. The operation to update extension at remote node fails.

However, to inter change extensions across HTTPS network it is recommended to perform following steps:

2. Perform sync across HTTPS network.
3. Change the extension of UserA to 1002 and UserB to 1000 on local node.
4. Perform sync across HTTPS network.
5. Change the extension of User A to 1001.
6. Perform sync across HTTPS network.
7. After performing step 3 to step 6, the extension of UserA and UserB are inter changed across HTTPS network.

How to Remove Orphan Objects from Unity Connection HTTPS network

Orphan objects: If the replication objects such as users, contacts and distribution list gets removed from the home location, but it does not get removed from the HTTPS linked location after completion of synchronization task, then the object is termed as orphan object on the HTTPS linked location.

Administrator can use the following steps to remove the Orphan objects of linked HTTPS location 'HTTPS-Location-2' from location 'HTTPS-Location-1'.

Following are the steps to remove Orphan objects from Unity connection

1. Enable the orphan object removal configuration by running following CLI from command prompt on locationHttps-Location-1.

   First fetch the object id of the configuration parameter "IsOrphanObjectDeletionEnable" from tbl_configuration.

dadmin:run cuc dbquery unitydirdb select objectid, fullname, value from vw_configuration where fullname='System.LocalNetwork.IsOrphanObjectDeletionEnable'

Using the objectId fetched in step 1.a and execute the following procedure to enable the orphan object removal configuration.

admin:run cuc dbquery unitydirdb execute procedure csp_configurationmodify(pobjectid='ObjectId', pvaluebool=1)

1. Perform Re-sync operation on HTTPS-Location-1 using Re-sync All buttons on the Networking > HTTPS Links > Search HTTPS Links page in Cisco Unity Connection Administration for the HTTPS-Location-2.

2. It is required to disable this configuration once the re-sync operation gets completed. To disable the configuration use the following command with the same objectId used in 1)a.

admin: run cuc dbquery unitydirdb execute procedure csp_configurationmodify(pobjectid='ObjectId', pvaluebool=0)
Received RTMT NetworkLoopDetected

If admin receives the RTMT alert NetworkLoopDetected then you can do below steps to rectify this scenario.

1. Configure Network Analyzer Tool for Https network. For more information on network analyzer, see the http://www.ciscounitytools.com/Applications/General/NetworkAnalyzer/NetworkAnalyzer.html.

2. Analyze the graphical view of the network to find the locations which are creating the loop.

3. Unjoin and join the concerned locations from the network in an appropriate topology to resolve the loop.

Sender Receives NDR When Sending Voice Message to Distribution List

When the membership information of the concerned distribution list has been updated recently and this membership information has not been replicated to the entire network, the receiving node may send NDR as it does not have the updated membership info.

Make sure that the updated membership information should be replicated to the entire network before sending voice-messages to this DL.

Troubleshooting Message Addressing

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.

If a message is successfully created and sent to a remote recipient but is not received by the recipient, see the Troubleshooting Message Transport.

Users Cannot Address Messages to Remote Users, Contacts, or System Distribution Lists

If Unity Connection users are unable to address messages to remote objects within a Unity Connection site or on a linked Unity Connection or Cisco Unity site, do the following tasks in the order presented:

1. Check for the presence of the remote object in Unity Connection 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 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.

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 Troubleshooting Cisco Unity Connection, on page 1 chapter.

Checking the Partition and Search Space Configuration for Addressing to Remote Objects

If you have only a single 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 Unity Connection site to another Unity 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 Unity Connection site and a Cisco Unity site, a partition is automatically created in the Unity 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 Unity Connection locations. In order for Unity 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 Unity Connection users. Note that the order a partition appears in a search space is important if users address messages by extension. If, for example, Unity Connection and Cisco Unity users have overlapping 4-digit extensions and you want Unity Connection users to be able to reach other Unity 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 Unity Connection partitions that contain the overlapping 4-digit extensions.

At a minimum, when a Unity 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.

### Checking 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 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 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 Unity Connection Users or System Distribution Lists**

If Cisco Unity users are unable to address messages to users on a Unity Connection site to which Cisco Unity is linked via an intersite link (also known as Unity Connection Networking), do the following tasks in the order presented:

1. Check for the presence of the Unity Connection user object as a Unity Connection Networking subscriber in the Cisco Unity Administrator. This indicates whether the Unity Connection user object has been replicated. If the object is not found, see the Troubleshooting Directory Synchronization for further troubleshooting steps.

2. If the problem involves addressing by extension, check to see if the Unity 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 Unity Connection User Extension Creation in Cisco Unity.

**Troubleshooting Unity Connection User Extension Creation in Cisco Unity**

When you link a Unity Connection site and a Cisco Unity site, the Unity 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 Unity 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 Unity Connection extensions to the Cisco Unity Dialing Domain. To do so, for each Unity 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 Unity 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 Unity 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 > Unity Connection Networking Profile page in Cisco Unity Administrator) in order to update the extensions.
It is also possible for a Unity 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 Unity Connection user object is created without an extension, Cisco Unity users are not able to address to the user by extension.

If the problem involves many user extensions on the same Unity 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.

Configuring the Partition that Cisco Unity Users Can Address To for a Cisco Unity Connection Location

**Step 1**
In Cisco Unity Connection Administration on the Unity 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 and select Save.

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 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.
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 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

Unity Connection uses SMTP to exchange voice messages with other systems. This includes VPIM messages, messages between users within a Unity Connection site, messages to users on a different Unity Connection site or on a Cisco Unity site, and messages sent to Unity Connection by IMAP clients or forwarded by Unity Connection to the relay address configured on the Message Actions page for a user.

In order for a Unity Connection system to exchange SMTP messages with other voice messaging systems or Unity 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 Unity Connection networking site, typically you create each VPIM location on only one Unity 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 Unity Connection server that homes the VPIM location for delivery. In this case, only this Unity Connection server needs SMTP connectivity (either directly or through a smart host) with the remote messaging system.

When a message is recorded by a Unity 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 Unity 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 Unity Connection to the correct server, and sends the message. The process is reversed when Unity 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.

Messages Sent from Users on One Unity Connection Location Not Received by Users on Another Unity Connection Location

In general, messages that are successfully addressed to a remote user 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 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 Unity Connection location of the sending user. To diagnose and correct this condition, see the Troubleshooting Directory Synchronization.
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 Using Diagnostic Traces for Troubleshooting, on page 1 section.

Replies to Messages Sent by Remote Senders 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 is successfully delivered.

Messages Sent from a VPIM Location Not Received by 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 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 Unity 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 Unity 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 Unity 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 Unity Connection location within the Unity 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.
Messages Sent from Unity Connection 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 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 Unity 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.

Troubleshooting Directory Synchronization

Use the troubleshooting information in this section if you are experiencing difficulties with directory synchronization either within a Unity Connection site (intraper site networking) or between sites (intersite networking).

Troubleshooting Directory Synchronization Within a Unity Connection Site

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 Unity Connection site.

Unique Sequence Numbers (USNs) Mismatched Between Locations

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

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 “Using the Voice Network Map Tool” chapter of the Administration Guide for Cisco Unity Connection Serviceability Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/serv_administration/b_11xcucservag.html.
Automatic Directory Replication is Stalled

Directory changes on one 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 Unity 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.

In most cases, the problem should resolve itself after the five minute time-out, at which point the receiving Unity 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.

Manual Directory Replication is Stalled

When an administrator initiates a manual push or pull of the directory between two Unity Connection locations, the Push Directory or Pull Directory status displayed on the Networking > Unity 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 Unity 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 Unity 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 Mismatched Between Locations

When an administrator initiates a manual push or pull of the directory between two 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.

Resynchronizing 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 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 only synchronize changes since the last cycle, unless you manually request a full re-synchronization.

On a Unity 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 4: Troubleshooting Tools for Intersite Replication Between Unity Connection Sites lists some of the tools you can use to collect information about the operation of the Feeder and Reader applications for intersite networking.

Table 4: Troubleshooting Tools for Intersite Replication Between Unity Connection Sites

<table>
<thead>
<tr>
<th>Networking</th>
<th>Application</th>
<th>Troubleshooting Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>Reader</td>
<td>• The Networking &gt; Links &gt; Intersite Links &gt; 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enable FeedReader micro trace levels 00, 01, 02, 03, 10, and 14. See the Using Diagnostic Traces for Troubleshooting, on page 1 section for instructions.</td>
</tr>
</tbody>
</table>
Troubleshooting Directory Synchronization Between a 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 only synchronize changes since the last cycle, unless you manually request a full resynchronization.

On the Unity Connection site gateway, you can configure the schedule on which the Reader (also referred to as the FeedReader in Unity 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 Unity 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 > Unity Connection Networking page. Note that unlike the Unity 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 5: Troubleshooting Tools for Intersite Replication Between Cisco Unity Connection and Cisco Unity 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>
<thead>
<tr>
<th>Networking</th>
<th>Application</th>
<th>Troubleshooting Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Feeder</td>
<td>• Enable Feeder micro trace levels 00, 01, 02, and 03. See the Using Diagnostic Traces for Troubleshooting, on page 1 section for instructions.</td>
</tr>
<tr>
<td>Digital Networking</td>
<td>CuReplicator</td>
<td>• Enable all levels of CuReplicator.</td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
<td>• Enable all levels of SMTP.</td>
</tr>
</tbody>
</table>

If you want to manually start an incremental update of the directory on either site, you can do so using the Sync button on the Networking > Links > Intersite Links page in Cisco Unity Connection Administration on the Unity Connection site gateway. To initiate a full resynchronization of the entire directory, use the Resync All button on the same page.
### Table 5: Troubleshooting Tools for Intersite Replication Between Cisco Unity Connection and Cisco Unity

<table>
<thead>
<tr>
<th>Application</th>
<th>Troubleshooting Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Reader</td>
<td>• The Networking &gt; Links &gt; Intersite Links &gt; 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.</td>
</tr>
<tr>
<td></td>
<td>• Enable FeedReader micro trace levels 00, 01, 02, 03, 10, and 14. See the Troubleshooting Cisco Unity Connection, on page 1 chapter for instructions.</td>
</tr>
<tr>
<td>Connection Feeder</td>
<td>• Enable Feeder micro trace levels 00, 01, 02, and 03. See the Troubleshooting Cisco Unity Connection, on page 1 chapter for instructions.</td>
</tr>
<tr>
<td>Cisco Unity Reader</td>
<td>• The Networking &gt; Unity 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.</td>
</tr>
<tr>
<td></td>
<td>• The Cisco Unity Reader logs operational and error messages to the Windows Application Event Log.</td>
</tr>
<tr>
<td></td>
<td>• 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 Unity 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Cisco Unity Feeder</td>
<td>• 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.</td>
</tr>
</tbody>
</table>
If you want to manually start an incremental update of the directory on either site, you can do so using the Sync button on the Networking > Links > Intersite Links page in Cisco Unity Connection Administration on the Unity Connection site gateway or using the Sync Now button on the Network > Unity 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 Unity Connection site gateway or the Total Sync button on the Network > Unity Connection Networking page in the Cisco Unity Administrator on the Cisco Unity site gateway.

Cross-Server Sign-In and Transfers

When a Unity Connection server is networked with other Unity 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.

Users Hear the Opening Greeting Instead of 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 Unity Connection Location page for the destination location.

• The user is not found in the search scope on the originating location. 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. 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 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 Unity 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 Unity Connection Port Usage Analyzer to help determine if port usage is becoming a problem for cross-server transfers.

**User ID and PIN 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.

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 Troubleshooting Cisco Unity Connection, on page 1 chapter.


**Callers Prompted to Leave a Message Instead of 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 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 Unity 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 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 Unity 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 Unity 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 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.

**Callers Hear a Prompt Indicating that 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 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 Troubleshooting Cisco Unity Connection, on page 1 chapter.
Callers Hear a Prompt Indicating that Call Cannot be Completed When Attempting to Transfer to a Remote User
Troubleshooting Cisco Unity Connection SRSV

Error Message Appears When Testing the Connectivity of Unity Connection with Branch

You may receive the following error messages on the Edit Branch page of Cisco Unity Connection Administration when you test the connectivity of Unity 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 Unity 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 Unity 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 Message for Appears on the Central Unity 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 Unity Connection server is correct.
Unable to login to 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 `utilisreset_application_ui_administrator_password` CLI command. For more information on this command, see the “Utils Commands” chapter of the Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 11.0(1) at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/11_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100_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 Unity 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 Unity Connection server and provisioning is done successfully.

Status of Provisioning Remains In Progress for a Long Time

If the status of provisioning on Connection Administration remains “In Progress” for a long time, consider the following:

- Check the network connectivity of the central Unity Connection server with the branch.

- Check whether the central Unity Connection server details are entered correctly on the branch.

- Check whether the Unity Connection Branch Sync Service is active on both central Unity Connection server and branch. For more information on the services required for Connection SRSV, see the “Managing Cisco Unity Connection Services” chapter of the Cisco Unified Serviceability Administration Guide, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/serv_administration/b_11xcucservag.html.

- Check whether the REST services are active on central Unity Connection server and branch.

Provisioning from the Central Unity Connection Server to Branch Not Working

If the provisioning of the users from the central Unity Connection server to the branch does not work, make sure that the license status at central Unity Connection server is not “Expire”. If the license status at central Unity Connection server is “Expire”, you need to install the required licenses for the central Unity Connection server to make the license status as “Compliance” and start provisioning. For more information on licensing requirements, see the “Managing Licenses” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.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 Unity 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 Unity Connection server.

• Make sure that the deleted user on the central Unity Connection server is not used on the branch. For example, if a branch user on Unity Connection is used as operator on Connection SRSV, make sure to change the operator at branch before deleting the user at central Unity Connection server.

• Make sure that the deleted distribution list on the central Unity 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 Unity Connection Branch Sync Service is active on the central Unity 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 Unity 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 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 Unity Connection server on Cisco Unity Connection SRSV Administration to resolve the problem.

Logs are Not Created or SRSV feature Not Working Properly

If the logs for the branch are not generated or the SRSV feature is not working properly, you may restart the Unity Connection Branch Sync Service and the REST APIs on both the branch and Unity 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 Unity Connection Server Moves to Violation State

If the central Unity Connection server moves to the Violation state, make sure that the number of licenses for the Unity Connection features, such as SpeechView and Connection SRSV, does not exceed its maximum limit. For more information on licensing, see the “Managing Licenses” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Non-Delivery Receipts (NDR) on the Central Unity Connection Server

If you are getting NDR on the central Unity 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 Unity 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 mailbox quota increased to receive further emails. For more information on NDR codes, refer to the Troubleshooting Non-Delivery Receipts, on page 79 chapter of this guide.
Troubleshooting Video Messaging

Error Message Appears When You Test the Connectivity of Video Services

You may receive the following error messages on the Edit Video Service page of Cisco Unity Connection Administration when you test the connectivity of Unity Connection with the video server:

• “Video Server cannot be contacted by pinging.”

If you receive the “Video Server cannot be contacted by pinging.” error message on the Tasks Execution Results page while testing connectivity of Unity Connection with the video server, make sure:

• The DNS server is up and running.

• The FQDN, IP address, or hostname of the video server entered on the Edit Video Service page is correct.

Note

If the DNS server is not available, make sure that you enter only the IP address in the Video Server Field and the Allow Self Signed Certificate for Video Servers check box is checked.

• The state of video server is active and running.

• The system firewall is not blocking ICMP protocol.

• “Video server is not responding on the port <port number>.“:

If you receive the “Video server is not responding on the port <port number>.” error message on the Tasks Execution Results page when you test the connectivity of the Unity Connection with video server, make sure that the port number entered on the Edit Video Service page is correct.

• “Username or password is incorrect.”:
If you receive the “Username or password is incorrect.” error message on the Tasks Execution Results page when you test the connectivity of the Unity Connection with video server, make sure that the username and password of video server entered on the Edit Video Service page are correct.

- “Failure in validating the video server certificates.”:

If you receive the “Failure in validating the video server certificates.” error message on the Tasks Execution Results page when you test the connectivity of the Unity Connection with video server, make sure:

- The DNS server is up and running.

- The valid video server certificates are uploaded on Unity Connection. If the valid video server certificates are not uploaded, make sure that the third-party video server certificates are uploaded and the Allow Self Signed Certificate for Video Server check box is not checked on the New Video Service page.

Note

If the DNS server is not available, make sure that you enter only the IP address in the Video Server field and the Allow Self Signed Certificate for Video Server check box is checked.

Error Message Appears When You Test the Connectivity of Video Service Account with Video Services

You may receive the following error messages on the Video Service Accounts Status page of Cisco Unity Connection Administration when you test the connectivity of the video service account (of a user) with video services:

- “The Enable Video settings are disabled for this user in the Edit Class of Service page.”

If you receive the “The Enable Video settings are disabled for this user in the Edit Class of Service page.” error message on the Tasks Execution Results page when you test the configuration of video service account with video services, make sure that you have selected the Enable Video settings in the Edit Class of Service page for that user.

- “Video service is disabled.”

If you receive the “Video service is disabled.” error message on the Tasks Execution Results page when you test the configuration of the video service account with video services, make sure that you have selected the Enabled option in the Edit Video Service page.

- You may receive the same error messages that appeared when testing the connectivity of Unity Connection with video server. For more information on error messages, see Error Message Appears When You Test the Connectivity of Video Services.

Unable to Establish Video Call through Telephone User Interface (TUI)

If a user login via direct sign-in using telephone user interface and is unable to establish a video call, check the following:
• The DNS server is up and running. If the DNS server is not available, make sure that you enter only the IP address in the Video Server field and the Allow Self Signed Certificate for Video Server check box is checked.

• Make sure that the Cisco Camera and Video Capabilities options are enabled for the device in Cisco Unified Communications Manager.

• Make sure that the state of video server is up and running using the Test button on the Edit Video Service page.

• Make sure that you have restarted the Connection Conversation Manager service after updating the video service.

• Check the connectivity of video service account (of a user) with video server.

• Check whether the Map Video Service option is enabled in video service account for the user.

• Check whether the H.264 video format (or codec) is advertised for integrating with video endpoint.

• Make sure that you integrate Unity Connection with Cisco Unified Communications Manager over SIP.

• Make sure that the root certificate of video server is uploaded in Tomcat-trust of Unity Connection.

• Make sure that each server in a Unity Connection cluster does not exceed the maximum of 25 concurrent video calls.

Unable to record Video greeting or message through Telephone User Interface (TUI)

If a user is unable to record video greetings or messages using telephone user interface, check whether the state of video server using the Test button on the Edit Video Service page.

Unable to playback Video greeting through Telephone User Interface (TUI)

If a user login via direct sign-in using telephone user interface and is unable to playback video greetings, consider the following:

• Check whether the state of video server is active and running using the Test button on the Edit Video Service page.

• Check whether the My Personal Recording option is enabled for video greetings in the Callers See section for the user.

• If the video file on video server is corrupted, re-record the video greeting. A video file is considered corrupted when the video greeting gets downgraded to audio during playback.

• If the response time from DNS is slow, the playback of two subsequent video greetings is delayed.

Unable to Play Video Greetings When Received Unanswered Call

In case of an unanswered call (“ring-no-answer”), if the called user is unable to play video greeting to the calling user, check the following:
• Whether the state of video server is active and running using the Test button on the Edit Video Service page.

• Check whether the video service account is created for a user.

• Check the connectivity of video service account (of a user) with video server.

• Check whether the My Personal Recording option is enabled for video greetings in the Callers See section for the user.

• Check whether the Outside Caller option is enabled in the Edit Class of Service page for the called user if the calling user is an unidentified caller.

### Video Call Downgrades to Audio while Recording/Playing Video Message

If the video call downgrades to audio with the “video services are not available, using audio for the duration of call” prompt while playing or recording the video message, check the following:

- Whether the state of video server is active and running using the Test button on the Edit Video Service page.

- Check the error codes sent by the video server.

### Video Playback Hangs in Between

If the video recording hangs while playback, do the following:

- Press # button on TUI to end the playback and continue with the call.

- Check the conversation logs to diagnose the issue.

### Troubleshooting Video Quality of Video Greetings and Messages

If the video quality is poor during the playback of video greeting or video message, check the following:

- Check and reduce the KeyFrame Requests interval mentioned in the **Interval in Seconds for sending KeyFrame Requests to End Point during recording** option. To do this, login to Cisco Unity Connection Administration, navigate to Advanced > Telephony and select **Interval in Seconds for sending KeyFrame Requests to End Point during recording**.

- Check and update the value of the session bit rate for video calls in the **Maximum Session Bit Rate for Video Calls in Cisco Unified Communications Manager** option depending on the video resolution settings the administrator have selected in Cisco Unity Connection Administration. To check and update the session bit rate, login to Cisco Unified Communications Manager, navigate to System > Region Information > Region, and update the value of **Maximum Session Bit Rate for Video Calls** field. To configure video resolution, login to Unity Connection Administration, navigate to Port Group > Port Group Basics > Change Advertising and update the value in the **Video Resolution** field.
Error Codes Send by Cisco MediaSense

Unity Connection integrates with Cisco MediaSense video server. You may receive the following error codes at RTMT tool from Cisco MediaSense.

Error Codes Received by Cisco MediaSense

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Applicable to</th>
</tr>
</thead>
<tbody>
<tr>
<td>E_MIU_MS_CONNECTOR_FAILURE</td>
<td>If there is no response or error in HTTP response from Cisco MediaSense.</td>
<td>At the time:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Establishing a video call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recording a video greeting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Playback of video greeting.</td>
</tr>
<tr>
<td>E_MIU_MS_AUTHENTICATION_FAILURE</td>
<td>Username or password is incorrect</td>
<td>At the time of establishing a video call using telephone user interface.</td>
</tr>
<tr>
<td>E_MIU_MS_REDIRECT_FAIL</td>
<td>If the redirect IP address or hostname is missing in the response, Cisco MediaSense sends response 3000.</td>
<td>At the time of establishing a video call using telephone user interface.</td>
</tr>
<tr>
<td>E_MIU_MS_SESSION_ID_NOT_FOUND</td>
<td>If the requested session ID is not available at Cisco Media Sense.</td>
<td>During playback of video greetings</td>
</tr>
<tr>
<td>E_MIU_MS_INTERNAL_FAILURE</td>
<td>If the unknown server error occurred, Cisco MediaSense sends response 5000.</td>
<td>At the time of establishing a video call</td>
</tr>
<tr>
<td>E_MIU_MS_ERROR_UNKNOWN</td>
<td>If any request to Cisco MediaSense fails.</td>
<td>At the time of establishing a video call</td>
</tr>
<tr>
<td>E_MIU_MS_RESPONSE_CODE_UNKNOWN</td>
<td>If there is no response code or the response code field is completely missing in the response from Cisco MediaSense.</td>
<td>At the time of establishing a video call</td>
</tr>
</tbody>
</table>

For troubleshooting the scenarios received at the time of establishing a video call, see the Unable to Establish Video Call through Telephone User Interface (TUI).

For more information on the error codes received from Cisco MediaSense, see the Cisco MediaSense Developer Guide.
Troubleshooting the Phone System Integration

Diagnostic Tools

There are diagnostic tools available to help you troubleshoot phone system integrations. For more information, see the sections below.

Configuring Unity Connection for the Remote Port Status Monitor

You can use the Remote Port Status Monitor for viewing the real-time 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 Unity 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/cxnportstatusmonitorcuc7x/portstatusmonitorcuc7x.html.

Configuring Unity Connection for the Remote Port Status Monitor

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unity Connection Administration, expand System Settings &gt; Advanced &gt; and select &gt; Conversations. On the Conversation Configuration page, check the Enable Remote Port Status Monitor Output check box.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations and select Save.</td>
</tr>
</tbody>
</table>

Note: You can enter up to 70 IP addresses. Each IP address must be separated from the following IP address by a comma.
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 Unity Connection are failing.
- Ports are failing to register.

Using 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

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.
- 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, on page 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 Integration Guide for Cisco Unity Connection at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Unity Connection Not Answering Any Calls

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

Verifying the Phone System Settings in Cisco Unity Connection Administration

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.

1. In the Task Execution Results window, select **Close**.

SUMMARY STEPS

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

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

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

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unity Connection Administration, expand <strong>Telephony Integrations</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Correct any incorrect values in Cisco Unity Connection Administration. If you change any values, select <strong>Save</strong> before leaving the page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If prompted to reset a port group, on the applicable Port Group Basics page, select <strong>Reset</strong>. Otherwise, continue to Step 5.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Related Links list, select <strong>Check Telephony Configuration</strong> and select <strong>Go</strong> to verify the phone system integration settings.</td>
</tr>
</tbody>
</table>

**Unity Connection Not Answering Some Calls**

When 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.

Following are the tasks to troubleshoot sporadic answers on incoming calls:

1. Confirm that the routing rules are working correctly. See the **Confirming Routing Rules**.

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**.

**Confirming Routing Rules**

By default, Unity Connection does not reject any calls. If routing rules have been changed, Unity 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, on page 1**.

**Confirming Voice Messaging Port Settings**

If the phone system is programmed to send calls to a voice messaging port on Unity Connection that is not configured to answer calls, Unity Connection does not answer the call.
## Confirming that Calls are Sent to the Correct Voice Messaging Ports on Cisco Unity Connection

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
2. On the Search Ports page, note which ports are designated to answer calls.
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.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Administration, expand <strong>Telephony Integrations</strong>, then select <strong>Port</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Search Ports page, note which ports are designated to answer calls.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Confirming that Voice Messaging Ports are Enabled

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
2. On the Search Ports page, review the Enabled column.
3. If a voice messaging port is not enabled and should be in use, select the display name of port.
4. On the Port Basics page for the port, check the **Enabled** check box to enable the port.
5. On the Port menu, select **Search Ports**.
6. Repeat **Step 3 through Step 5** for all remaining ports that should be in use.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Administration, expand <strong>Telephony Integrations</strong>, then select <strong>Port</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Search Ports page, review the Enabled column.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If a voice messaging port is not enabled and should be in use, select the display name of port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Port Basics page for the port, check the <strong>Enabled</strong> check box to enable the port.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the Port menu, select <strong>Search Ports</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat <strong>Step 3 through Step 5</strong> for all remaining ports that should be in use.</td>
</tr>
</tbody>
</table>
Troubleshooting an Integration of Unity Connection with Cisco Unified Communications Manager

Viewing or Editing IP Address of Cisco Unified Communications Manager

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand Telephony Integrations > and select Port Group.
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.
3. On the Port Group Basics page, on the Edit menu, select Servers.
4. On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and select Save.
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.
6. On the Port Group Basics page, under Port Group, select Reset.

DETAILED STEPS

Step 1  In Cisco Unity Connection Administration, expand Telephony Integrations > and 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 Repeatedly Disconnected in an SCCP Integration

When the Unity Connection voice messaging ports do not register with Cisco Unified CM in an SCCP integration, or if the Unity 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.

Following are the tasks to troubleshoot port registration problems:

1. Test the port group. See the Testing the Port Group.
2. Confirm that another port group on the Unity 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 Not Using the Same Device Name Prefix.
3. Confirm that another Unity 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 Unity Connection Server Not Using the Same Device Name Prefix.
Testing the Port Group

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port Group.
2. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
3. On the Port Group Basics page, in the Related Links list, select Test Port Group and select Go.
4. When prompted that the test terminate all calls in progress, select OK.
5. Follow the steps for correcting the problems.
6. Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

DETAILED STEPS

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

Step 4  When prompted that the test 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.

If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test fails. 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 Not Using the Same Device Name Prefix

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port Group.
   On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
2. On the Port Group Basics page, note the value of the Device Name Prefix field.
3. Select Next to view the next port group for which the integration method is SCCP (Skinny).
4. If the value of the Device Name Prefix field is different from the value that you noted in **Step 2**, skip to **Step 7**. 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.

5. Select **Save**.

6. Select **Reset**.

7. Repeat **Step 3** through **Step 6** for all remaining port groups for which the integration method is SCCP (Skinny).

**DETAILED STEPS**

**Step 1**

In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

**Step 2**

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

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

**Step 4**

If the value of the Device Name Prefix field is different from the value that you noted in **Step 2**, skip to **Step 7**. 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 5**

Select **Save**.

**Step 6**

Select **Reset**.

**Step 7**

Repeat **Step 3** through **Step 6** for all remaining port groups for which the integration method is SCCP (Skinny).

**Confirming that Another Unity Connection Server Not Using the Same Device Name Prefix**

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration on the first Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

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

3. In Cisco Unity Connection Administration on the second Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

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

5. If the value of the Device Name Prefix field is different from the value you noted on the first Unity Connection server in **Step 2**, 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.

6. Select **Save**.

7. Select **Reset**.

8. Select **Next**.

9. Repeat **Step 5** through **Step 8** for all remaining port groups for which the integration method is SCCP (Skinny).
DETAILED STEPS

Step 1: In Cisco Unity Connection Administration on the first Unity Connection server, expand Telephony Integrations, then select Port Group. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 2: On the Port Group Basics page, note the value of the Device Name Prefix field.

Step 3: In Cisco Unity Connection Administration on the second Unity Connection server, expand Telephony Integrations, then select Port Group. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 4: On the Port Group Basics page, note the value of the Device Name Prefix field. 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 5: If the value of the Device Name Prefix field is different from the value you noted on the first Unity Connection server in Step 2, 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: Select Next.

Step 9: Repeat Step 5 through Step 8 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 using the command-line interface (CLI), enter show network ipv6 settings.
   • To check using Cisco Unified Operating System Administration, see the Confirming that IPv6 is Enabled Using Cisco Unified Operating System Administration.

2. Confirm that Unity Connection is configured to use the appropriate addressing mode and preferences. See the Confirming the IPv6 Addressing Mode and Preferences Settings

3. If you have configured an IPv6 host name for the Unity 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 using the CLI, enter utils network ipv6 ping <IPv6 host name>.

4. If you have configured the port group(s) in Unity 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 Unity

Confirming that IPv6 is Enabled Using Cisco Unified Operating System Administration

**SUMMARY STEPS**

1. In Cisco Unified Operating System Administration, Settings > IP and select **Ethernet IPv6**.
2. On the Ethernet IPv6 Configuration page, review the **Enable IPv6** check box, and check it if it is not already checked.
3. If you checked the Enable IPv6 check box in Step 2, configure the Address Source for the Unity Connection server. To apply the change, check Update with Reboot, and select **Save**. The Unity Connection server reboots in order for the change to take effect.

**DETAILED STEPS**

**Step 1**
In Cisco Unified Operating System Administration, Settings > IP and 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 Unity Connection server. To apply the change, check Update with Reboot, and select **Save**. The Unity Connection server reboots in order for the change to take effect.

Confirming the IPv6 Addressing Mode and Preferences Settings

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.
2. On the Edit General Configuration page, review the option selected for **IP Addressing Mode**, which controls where Unity Connection listens for incoming traffic:
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.
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:

**DETAILED STEPS**

**Step 1**
In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.
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 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 Faced When Unity Connection is Configured for Cisco Unified Communications Manager Authentication or Encryption

If problems occur when 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


Follow the tasks to troubleshoot problems when Cisco Unified CM authentication or encryption is configured:
1. Confirm that the Cisco Unified CM CTL client is configured for mixed mode. See the Confirming that Cisco Unified Communications Manager CTL Client is Configured for Mixed Mode.

2. Test the port group configuration. See the Testing the Port Group Configuration.

3. For SCCP integrations, confirm that the security mode setting for the ports in Unity Connection matches the security mode setting for the ports in Cisco Unified CM. See the Matching the Security Mode Setting for Ports in Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only).

4. For a SIP trunk integration, confirm that the security mode setting for the Unity 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 Unity Connection Port Group and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 133 section.

5. For SIP trunk integrations, confirm that the Subject Name field of the Unity 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 Unity Connection SIP Certificate and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 133 section.

6. For SIP trunk integrations, confirm that Unity Connection and the SIP trunk use the same port. See the Matching the Port Used by Unity Connection SIP Security Profile and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 133 section.

7. Copy the Unity Connection root certificate to the Cisco Unified CM servers. See the Copying the Unity Connection Root Certificate to Cisco Unified Communications Manager.

---

**Confirming that Cisco Unified Communications Manager CTL Client is Configured for Mixed Mode**

**SUMMARY STEPS**

1. In Cisco Unified Communications Manager Administration, on the System menu, select **Enterprise Parameters**.
2. On the Enterprise Parameters Configuration page, under Security Parameters, locate the **Cluster Security Mode** field.
3. Confirm that the setting is 1, which means that the CTL client is configured for mixed mode.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified Communications Manager Administration, on the System menu, select <strong>Enterprise Parameters</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Enterprise Parameters Configuration page, under Security Parameters, locate the <strong>Cluster Security Mode</strong> field.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Confirm that the setting is 1, which means that the CTL client is configured for mixed mode.</td>
</tr>
</tbody>
</table>

**Testing the Port Group Configuration**

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.
2. On the Search Port Groups page, select the name of a port group.
3. On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.
4. When prompted that the test terminates all calls in progress, select **OK**.
5. Follow the steps for correcting the problems.
6. Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Search Port Groups page, select the name of a port group.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Port Group Basics page, in the Related Links list, select Test Port Group and select Go.</td>
</tr>
</tbody>
</table>

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

| Step 4 | When prompted that the test terminates all calls in progress, select OK. The Task Execution Results displays one or more messages with troubleshooting steps. |

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Follow the steps for correcting the problems.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test fails. You must configure Cisco Unified CM and the system to enable pings so that the test can accurately test the port registration.</td>
</tr>
</tbody>
</table>

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

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

SUMMARY STEPS

1. In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select Cisco Voice Mail Port. On the Find and List Voice Mail Ports page, select Find.
2. In the Device Security Mode column, note the security mode setting for the ports.
3. In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port.
4. On the Search Ports page, select the name of the first port.
5. On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 2 and select Save.
6. Select Next.
7. Repeat Step 5 and Step 6 for all remaining ports.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select Cisco Voice Mail Port. On the Find and List Voice Mail Ports page, select Find.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Device Security Mode column, note the security mode setting for the ports.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Search Ports page, select the name of the first port.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 2 and select Save.</td>
</tr>
</tbody>
</table>
Step 6 Select Next.
Step 7 Repeat Step 5 and Step 6 for all remaining ports.

Matching the Security Mode Setting for Unity Connection Port Group and 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 In Cisco Unity Connection Administration, expand Telephony Integrations, then select Port Group.
Step 6 On the Search Port Groups, select the name of the applicable port group.
Step 7 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 Unity Connection SIP Certificate and 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 In Cisco Unity Connection Administration, expand Telephony Integrations > Security, then select SIP Certificates.
Step 6 On the Search SIP Certificates page, select the name of the SIP certificate.
Step 7 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 Unity Connection SIP Security Profile and 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 In Cisco Unity Connection Administration, expand Telephony Integrations > Security, then select SIP Security Profile.
Step 6 On the Search SIP Security Profiles page, select the name of the SIP security profile with "TLS."
Step 7 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 Unity Connection Root Certificate to Cisco Unified Communications Manager

Copying the Root Certificate for Cisco Unified Communications Manager 4.x

Procedure

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.
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**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.
4. In the Filename field, confirm that the extension is **.0** (rather than **.htm**), and select **Save**.
5. In the Download Complete dialog box, select **Close**.
6. Copy the 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.
7. In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the Unity Connection to the Cisco Unified CM servers.

DETAILED STEPS

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 Unity Connection server where you want to save the Unity Connection root certificate as a file.

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

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

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

Step 6 Copy the 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 Unity Connection to the Cisco Unified CM servers.

Copying the Root Certificate for Cisco Unified Communications Manager 5.x

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.
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**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.

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

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

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

7. If prompted, restart the Unity Connection software.

**DETAILED STEPS**

**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 Unity Connection server where you want to save the Unity Connection root certificate as a file.

**Step 4**
In the Filename field, confirm that the extension is .pem (rather than .htm), and select Save. The certificate must be saved as a file with the extension .pem (rather than .htm) or Cisco Unified CM does not recognize the certificate.

When 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 do not function correctly.

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

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

The 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 does not let the Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Unity Connection device certificates.


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

c) Browse to the 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 Unity 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 Unity Connection software.
Copying the Root Certificate for Cisco Unified Communications Manager 6.x, 7.x, and Later

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security > Root Certificate**.
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**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.
4. In the Filename field, confirm that the extension is .pem (rather than .htm), and select **Save**.
5. In the Download Complete dialog box, select **Close**.
6. Copy the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

**DETAILED STEPS**

---

**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 Unity Connection server where you want to save the Unity Connection root certificate as a file.

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

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

When 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 do not function correctly.

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

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

The 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 does not let the Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Unity 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 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 Unity 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.

Troubleshooting PIN Synchronization between Unity Connection and Cisco Unified CM

This chapter explains various problems that may occur while using PIN Synchronization feature along with the resolution.

Unable to Update PIN through Cisco Unity Connection Administration or Cisco PCA

While updating the voicemail PIN through Cisco Unity Connection Administration and Cisco Personal Communications Assistant (CPCA) with PIN Synchronization feature enabled, you may receive any of the following error messages:

• "Failed to update PIN on CUCM. Reason: Trivial credential"
• "Failed to update PIN on CUCM: Invalid credential length"
• "Failed to update PIN on CUCM. Reason: Duplicate credential found in history"

If you receive the above error messages, make sure that you entered a valid PIN as per the Credential Policy Configuration on Cisco Unified CM.

• "Bad response from CUCM. Reason: Requested resource is not available"

If you receive the "Bad response from CUCM. Reason: Requested resource is not available " error message, verify that:

• The username and password of primary AXL server entered on the Edit AXL Servers page are correct.
• The AXL server is up and running.

To verify this, in Cisco Unity Connection Administration, navigate to Telephony Integration > Phone System and select the Phone System associated with the user. On the Phone System Basics page, navigate to Edit > Cisco Unified Communication Manager AXL Servers. On the Edit AXL Server page, select Test under section AXL Servers.

• Proper tomcat certificates are uploaded for the AXL server.

To verify this, on the Edit AXL Server page, select Test under section AXL Servers. To ignore the certificate validation errors, check the Ignore Certificate Errors check box on the Edit AXL Servers page.

• "Failed to update PIN on CUCM. Reason: Error getting the pin"

If you receive the "Failed to update PIN on CUCM. Reason: Error getting the pin" error message, make sure that the publisher server of Cisco Unified CM is up and running.
Unable to Update PIN through Telephone User Interface (TUI)

With PIN Synchronization feature enabled, if a user hears the "Your PIN has not been changed, for help press 0 or contact to your system administrator" error prompt while updating the phone PIN through TUI, you must verify the following:

- The username and password of primary AXL server entered on the Edit AXL Servers page are correct.
- The AXL server is up and running. To verify this, select Test on the Edit AXL Server page.
- Either Unity Connection has successfully validated the certificates for AXL server or Ignore Certificate Errors check box is checked on the Edit AXL Servers page.
- Authentication Rules on Cisco Unity Connection Administration are same as the Credential Policy Configuration on Cisco Unified CM and.
- A user has entered the valid PIN as per the credential policies.
- The publisher server of Cisco Unified CM is up and running.

Using Traces for PIN Synchronization

You can use Unity Connection traces to troubleshoot PIN Synchronization problems. You need to enable the following micro traces to troubleshoot the problems:

<table>
<thead>
<tr>
<th>Error Scenario</th>
<th>Traces to set</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN synchronization is failed on Cisco Unity Connection Administration</td>
<td>Cuca (all levels)</td>
</tr>
<tr>
<td>PIN synchronization is failed on Cisco PCA</td>
<td>CiscoPCA (level 00,01,02,13)</td>
</tr>
<tr>
<td>PIN synchronization is failed through Telephone User Interface</td>
<td>CDL (level 10 and 11) and ConvSub (level 01,03,04,05)</td>
</tr>
<tr>
<td>PIN synchronization is failed through API</td>
<td>VMREST (all levels)</td>
</tr>
<tr>
<td>PIN synchronization is failed through Bulk Administration Tool</td>
<td>Bulk Administration Tool (all levels)</td>
</tr>
<tr>
<td>AXL server issues</td>
<td>AxlAccess (level 00,01)</td>
</tr>
<tr>
<td>Certificate validation issues</td>
<td>Cuca (all levels)</td>
</tr>
</tbody>
</table>

For detail instructions on enabling and collecting diagnostic traces, see the Using Diagnostic Traces for Troubleshooting section.
Troubleshooting Message Waiting Indicators (MWIs)

Triggers for Turning MWIs On and Off

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 Unity Connection to turn MWIs on and off:

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

Any message that arrives on the Unity Connection message store (for example, voice messages, emails, and faxes) trigger turning MWIs on and off.

• When the user saves or deletes a read message, Unity Connection notifies the phone system to turn off the MWI on the phone.

• When a user deletes a new message without listening to it, Unity Connection notifies the phone system to turn off the MWI on the phone.

• When MWIs are synchronized, Unity 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.

• The user listens the entire message. You can perform either of the following to turn off the MWI:
  • Save or Delete the message after listening it.
  • In Cisco Unity Connection Administration, Select Users. On the Search Users page, Select the alias of the user. On the Edit User Basics page of the user, navigate Edit > Playback Message Settings. On the Playback Message Settings page, Select Saved under When Disconnected or User Hangs Up During Message Playback field.

• In an email application, in the Web Inbox, or Messaging Inbox , the user marks a listened-to message as unread.

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

**MWI Problems**

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

**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.

Following are the tasks to troubleshoot when MWIs do not turn on or off:

1. Run the Check Telephony Configuration test. See the Running the Check Telephony Configuration Test.

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**

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 Cisco Unity Connection Administration, select Telephony Integrations > 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 Cisco Unity Connection Administration, select Telephony Integrations > Ports.

5. Confirm that the port groups for the phone system integration enable MWIs. To view the Enable Message Waiting Indicators check box, in Cisco Unity 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 Unity Connection settings, in Cisco Unity 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 Integration Guide for Cisco Unity Connection 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 Cisco Unity 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 Cisco Unity 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 Cisco Unity 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 Unity Connection server was upgraded, restored using the Disaster Recovery System, or experienced an event that disrupted MWI synchronization. See the Synchronizing MWIs.

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 Troubleshooting Cisco Unity Connection, on page 1 chapter.

Running the Check Telephony Configuration Test

---

Note

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

Procedure
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 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.

### Synchronizing MWIs for a Phone System Integration

**Procedure**

Step 1
In Cisco Unity Connection Administration, expand **Telephony Integrations** and select **Phone System**. On the Search Phone Systems page, select the name of the phone system for which you want to synchronize all MWIs.

Step 2
On the Phone System Basics page, under Message Waiting Indicators, select **Run**.

**Note** 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 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 **Confirm that Unity Connection Uses Port Memory (PIMG/TIMG Integrations)**.

- 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 Unity 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)**.
Confirm that 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 Unity 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
This problem does not apply to PIMG/TIMG serial integrations.

Step 1
In Cisco Unity Connection Administration, expand Telephony Integrations > and 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 and select Save.

Deleting or Reconfiguring MWI Ports When Port Memory is Used (PIMG/TIMG Integrations)

If 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.

Step 1
In Cisco Unity Connection Administration, expand Telephony Integrations and select Phone System. On the Search Phone Systems page, select the name of the phone system.
Step 2
On the Phone System Basics page, under Message Waiting Indicators, check the Force All MWIs Off for This Phone System check box and select Save. All MWIs for the phone system are turned off.
Step 3
In the left pane, select Port.
Step 4
On the Search Ports page, check the check boxes of the MWI ports that you want to delete and select Delete Selected.
Step 5
In the left pane, select Phone System. On the Search Phone Systems page, select the name of the phone system.
Step 6
On the Phone System Basics page, under Message Waiting Indicators, uncheck the Force All MWIs Off for This Phone System check box and select Save.
Step 7
To the right of Synchronize All MWIs on This Phone System, select Run. All MWIs for the phone system are synchronized.

Reconfiguring MWI Ports When Port Memory is Used (PIMG/TIMG Integrations)

Step 1
In Cisco Unity Connection Administration, expand Telephony Integrations > and select Phone System. On the Search Phone Systems page, select the name of the phone system.
Step 2
On the Phone System Basics page, under Message Waiting Indicators, check the Force All MWIs Off for This Phone System check box and select Save. All MWIs for the phone system are turned off.
Step 3
In the left pane, select Port. On the Search Ports page, select the display name of the first MWI port that you want to reconfigure not to set MWIs.
Step 4
On the Port Basics page, under Port Behavior, enter the applicable settings and select Save.
Step 5
If there are more MWI ports that you want to reconfigure not to set MWIs, select Next. Otherwise, skip to Step 7.
Step 6
Repeat Step 4 and Step 5 for all remaining MWI ports that you want to configure not to set MWIs.
Step 7  In the left pane, select **Phone System**.

Step 8  On the Search Phone Systems page, select the name of the phone system.

Step 9  On the Phone System Basics page, under Message Waiting Indicators, uncheck the **Force All MWIs Off for This Phone System** check box and select **Save**.

Step 10 To the right of Synchronize All MWIs on This Phone System, select **Run**. All MWIs for the phone system are synchronized.

### 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**.

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)**.

### Determining the MWI Port Activity

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In Cisco Unity Connection Serviceability, on the Tools menu, select <strong>Reports</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>On the Serviceability Reports page, select <strong>Port Activity Report</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>On the Port Activity Report page, select the applicable options for the report.</td>
</tr>
<tr>
<td>4</td>
<td>Select <strong>Generate Report</strong>.</td>
</tr>
</tbody>
</table>

### 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.

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of the first port group for the SCCP integration.

2. 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.

3. 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 and select **Save**.

4. Select **Next**.

5. Repeat **Step 2** through **Step 3** for the remaining port groups in the SCCP integration.
No Message Count Sent on Phone When MWI is On

For Cisco Unified CM integrations, 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.

Enabling Message Counts for the Applicable New Messages

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand Users and select Users. On the Search Users page, select the alias of the applicable user.


3. On the Playback Message Settings page, under For New Messages, Play, check the applicable check boxes:

4. Select Save.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand Users and select Users. On the Search Users page, select the alias of the applicable user.

Step 2 On the Edit User Basics page, on the Edit menu, select Playback Message Settings.

Step 3 On the Playback Message Settings page, under For New Messages, Play, check the applicable check boxes:

- **Message Count Totals**—Unity Connection announces the total number of messages that are marked new, including voice, email, and fax messages.

- **Voice Message Counts**—Unity Connection announces the total number of voice messages that are marked new.

- **Email Message Counts**—Unity Connection announces the total number of email messages that are marked new.

- **Fax Message Counts**—Unity Connection announces the total number of fax messages that are marked new.

- **Receipt Message Counts**—Unity Connection announces the total number of receipts that are marked new.

Step 4 Select Save.

Incorrect Message Count and False MWI Notification Sent on Phone

If a user gets MWI on and there is no new voice messages in the mailbox of the user. The user may get this issue in the following scenarios:

**Scenario 1:**

Users may have same MWI Extension and different primary extension in a Phone System

If two or more users have different primary extension and same MWI extension within a Phone System, any of the user will get false MWI notification and incorrect message count on the phone. For example, a user A has primary extension and MWI extension as 1001 and another user B has primary extension 1002 and MWI
extension as 1001. If user B gets a new voice message, the MWI notification turns on for extension 1001, which is the primary extension of the user A. Hence user A also gets MWI notification but there is no new message in his mailbox.

To stop the false MWI notification on the phone, do the following:

• Execute the below command to identify the users having same MWI extension.

```sql
run cuc dbquery unitydirdb select u.alias, n.mwiextension from tbl_notificationmwi n inner join vw_user u on n.subscriberobjectid=u.objectid where n.mwiextension='<Extension on which user get false MWI notification>'
```

Example: If user gets false MWI notification on extension 1001, the command will be

```sql
run cuc dbquery unitydirdb select u.alias, n.mwiextension from tbl_notificationmwi n inner join vw_user u on n.subscriberobjectid=u.objectid where n.mwiextension= 1001
```

• On the Search Users page of Cisco Unity Connection Administrator, check the primary extension of the users that have same MWI extension.

The configuration is incorrect for the user, which have different primary and MWI extension. This causes the false MWI notification on the phone.

• To change the MWI extension of the user, go to Edit User Basics page of that user and navigate Edit > Message Waiting Indicators. In Extension field of Edit Message Waiting Indicators page, update the correct extension for MWI notification.

**Scenario 2**

User may exist in different partition having same primary extension

If two or more users have same primary extension in different partition, one of the user will get the false MWI notification on the phone. For example, a user A has primary as well as MWI extension as 1001 in partition A and other user B also has same extension 1001 as primary and MWI extension in partition B. If user B gets a new voice message, the MWI notification turns on for extension 1001, which is also the MWI extension of user A. Hence user A gets false MWI notification on the phone.

To stop the false MWI notification in different partition, do the following:

• Execute the below command to get the list of extension numbers and number of users corresponding to each extension (dtmfaccessid)

```sql
run cuc dbquery unitydirdb select first 10 dtmfaccessid,count(dtmfaccessid) from vw_user group by dtmfaccessid order by count(dtmfaccessid) desc
```

• Execute the below command to get the alias of the users having same extension (dtmfaccessid)

```sql
run cuc dbquery unitydirdb select first 10 dtmfaccessid,count(dtmfaccessid),alias from vw_user group by dtmfaccessid,alias order by count(dtmfaccessid)
```

• Check the Phone System associated with the users having same extension on Edit User Basics page of the users.

• If the users have same Phone System then select the different Phone System for each user through Edit User Basics page of Cisco Unity Connection Administrator.
Troubleshooting Audio Quality

Troubleshooting Audio Quality Using Check Telephony Configuration Test

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

**Using the Check Telephony Configuration Test to Troubleshoot Audio Quality**

**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**

Use the troubleshooting information in this section if the audio you hear from Unity Connection is choppy. Consider the following possible causes:

- The hard disk from which Unity Connection is playing a recording is full. To resolve the situation, eliminate unnecessary files from the hard disk.

- The network Unity Connection to the Unity Connection server is not adequate. To resolve the situation, improve the network Unity Connection.
• The Unity 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.

• You can check if there are any VMware snapshots. If yes, remove the snapshots.

• Stratum of NTP should be less than 5. You can check the stratum using the `utils ntp status` command.

• Toggle the settings for Audio Normalization for Recordings and Messages and Noise Reduction Settings on port group > Advanced Settings page.

**Problem with Garbled Recordings**

Use the troubleshooting information in this section if recordings sound garbled. See the following possible scenarios:

• The audio stream sounded garbled when Unity Connection created the recording. See the Troubleshooting a Garbled Audio Stream in the Network.

• The audio stream did not sound garbled when Unity Connection created the recording, but became garbled later. See the Troubleshooting How Unity Connection Makes Recordings.

**Troubleshooting a Garbled Audio Stream in the Network**

When the audio stream is garbled when Unity Connection created the recording, use the following task list to determine the cause and to resolve the problem.

Follow the tasks to troubleshoot a garbled audio stream in the network:

1. Confirm that the Unity Connection to the caller is clear. Calls that have bad PSTN connections or calls from mobile phones may sometimes have garbled audio streams. Unity 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 Unity 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 Unity Connection server by obtaining a sniffer capture at that point. If the audio stream from the sniffer capture is not garbled, Unity Connection may not be handling the audio stream correctly. See the Troubleshooting How Unity Connection Makes Recordings.

**Troubleshooting How Unity Connection Makes Recordings**

When the audio stream did not sound garbled when Unity Connection created the recording, but became garbled later, use the following task list to determine the cause and to resolve the problem.

Follow the tasks to troubleshoot how 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 Diagnostic Traces for Troubleshooting, on page 1.


3. Contact Cisco TAC.

**Problem with Garbled Prompts on Phone**

When 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.

Follow the tasks to troubleshoot 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 Unity 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 Unity 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 Unity Connection server by obtaining a sniffer capture at that point. If the audio stream from the sniffer capture is not garbled, Unity 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 Diagnostic Traces for Troubleshooting, on page 1.


6. Contact Cisco TAC.

**Problem with Volume of Recordings**

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 Unity Connection Recordings.

• Disable automatic gain control (AGC) for Unity Connection so that Unity Connection does not automatically adjust the volume of recordings. See the Disabling Automatic Gain Control (AGC) for Unity Connection.

• If the recordings do not have any sound, confirm that the advertised codec settings are correct. See the Confirming the Advertised Codec Settings, on page 150.

### Changing the Volume for Unity Connection Recordings

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

**Step 2**
On the Edit General Configuration page, in the Automatic Gain Control (AGC) Target Decibels field, enter the applicable number and select Save.

**Note**
AGC decibel levels are set in negative numbers. For example, –26 db is louder than –45 db.

### Disabling Automatic Gain Control (AGC) for Unity Connection

**Step 1**
In Cisco Unity Connection Administration, expand Telephony Integrations > and select Port Group. On the Search Port Groups page, select the name of the applicable port group.

**Step 2**
On the Port Group Basics page, in the Edit menu, select Advanced Settings.

**Step 3**
On the Edit Advanced Settings page, under Automatic Gain Control (AGC) Settings, uncheck the Enable AGC check box and select Save.

### Confirming the Advertised Codec Settings

**Verifying the Advertised Codec Settings**

**Step 1**
In Cisco Unity Connection Administration, expand Telephony Integrations and select Port Group. On the Search Port Groups page, select the name of the applicable port group.

**Step 2**
On the Port Group Basics page, under Advertised Codec Settings, determine whether the list of codecs is correct.

**Step 3**
If the list is correct, skip to Step 7. Otherwise, select Change Advertising.

**Step 4**
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, Unity 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, Unity 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 5** Select Save.

**Step 6** On the Edit menu, select Port Group Basics.

**Step 7** 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**

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 Diagnostic Traces for Troubleshooting, on page 1.
Using Traces to Troubleshoot Audio Quality Issues
Troubleshooting Notification Devices

Overview

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

When message notification through phones is slow for multiple users, use the following task list to determine the cause and to resolve the problem.

Following are the tasks to troubleshoot slow message notifications through phones for multiple users:

1. Confirm that ports are not too busy to handle message notification. See the Ports Too Busy to Make Notification Calls Promptly.

2. Confirm that there are enough ports assigned to message notification. See the Not Enough Ports Set for Message Notification Only.

3. Confirm that the phone system sends calls to ports that are set to answer calls. See the Confirm that Phone System Sends Calls to the Ports Set to Answer Calls.

Ports 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.
Reviewing 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 Set for Message Notification Only**

When a small number of ports are set to make notification calls and 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.

Determining if Number of Message Notification Ports is Adequate

**Step 1** In Cisco Unity Connection Serviceability, expand *Tools* and select *Reports*.
**Step 2** On the Serviceability Reports page, select *Port Activity Report*.
**Step 3** On the Port Activity Report page, select the applicable file format for the report output.
**Step 4** Set a date range by selecting the beginning and ending month, day, year, and time.
**Step 5** Select *Generate Report*.
**Step 6** View the report output, depending on the file format that you chose in **Step 3**.
**Step 7** 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 8** 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.

Confirm that Phone System Sends Calls to the Ports Set to Answer Calls

If the phone system is programmed to send calls to a port on Unity Connection that is not configured to answer calls, it is possible for a call collision to occur, which can freeze the port.

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

**Step 1** In Cisco Unity Connection Administration, expand *Telephony Integrations* > and select *Port*.
**Step 2** 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 3  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 2.

Step 4  On the Port Basics page, under Phone System Port, select Restart.

Step 5  When prompted that restarting the port terminates any call that the port is currently handling, select OK.

Step 6  Repeat Step 3 through Step 5 for all remaining ports that you changed in Step 2.

Message Notification Slow for a User

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:

1. The user settings may not be adequate for the needs of the user. See the Message Notification Setup is Inadequate.

2. The user settings may need adjustment to more correctly map to the work schedule of the user. See the Notification Attempts are Missed.

3. The user may not clearly understand how repeat notifications are handled by Cisco Unity Connection. See the Repeat Notification Option is Misunderstood.

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.

Determining Whether Notification Setup is Adequate

Step 1  In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, in the Search Results table, select the alias of the applicable user.

Step 2  On the Edit User Basics page, on the Edit menu, select Notification Devices.

Step 3  On the Notification Devices page, select the display name of the correct notification device.

Step 4  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 Unity Connection to call, ask the user if there is an alternate device to use for message notification.

Step 5  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.


### Resolving Missed Notification Attempts

**Step 1**  
In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, in the Search Results table, select the alias of the applicable user.

**Step 2**  
On the Edit User Basics page, on the Edit menu, select **Notification Devices**.

**Step 3**  
On the Notification Devices page, select the display name of the correct notification device.

**Step 4**  
On the Edit Notification Device page, check the **Repeat Notification If There Are Still New Messages** check box.

**Step 5**  
If the user has another notification device available, for **On Notification Failure**, select **Send To**, and select the device.

**Note**  
Because Unity Connection does not detect notification failure for SMTP devices, the **On Notification Failure** field is not available for notification devices of this type.

**Step 6**  
For phone or pager notification devices, in the Busy Retry Limit and RNA Retry Limit fields, increase the numbers so that Unity Connection makes more notification calls when the device does not answer or is busy.

**Step 7**  
For phone or pager notification devices, in the Busy Retry Interval and RNA Retry Interval fields, decrease the numbers so that Unity Connection makes notification calls more often when the device does not answer or is busy.

**Step 8**  
Select **Save**.

**Step 9**  
If you chose another device in **Step 5**, 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 and select **Save**.

**Step 10**  
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 Unity 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 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 Unity Connection restart notification each time a new message arrives, setting a long interval between repeat notification calls may lead the user to believe that Unity Connection is delaying notification.

### Resolving a Repeat Notification Problem

**Step 1**  
In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, in the Search Results table, select the alias of the applicable user.

**Step 2**  
On the Edit User Basics page, on the Edit menu, select **Notification Devices**.

**Step 3**  
On the Notification Devices page, select the display name of the correct notification device.

**Step 4**  
On the Edit Notification Device page, in the Notification Repeat Interval box, set a shorter interval, such as 15 minutes and select **Save**.
Message Notification Not Working at All

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:

- **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 Disabled or the Schedule Inactive.

Confirm that message notification is enabled for the correct types of messages. See the Only Certain Types of Messages Set to Trigger Notification.

- **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 Incorrect or Access Code for an External Line Missing (Phone and Pager Notification Devices Only).

Confirm that the notification device is assigned to the correct phone system. See the Message Notification Not Working at All, on page 157 section.

- **For SMS notification devices:** See the SMS Notifications Not Working for additional troubleshooting steps.

- **For SMTP notification devices:** See the SMTP Message Notification Not Working at All for Multiple Users for additional troubleshooting steps.

Notification Device Disabled or the Schedule 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.

Verifying a Device Status and Schedule

- **Step 1** In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, in the Search Results table, select the alias of the applicable user.
- **Step 2** On the Edit User Basics page, on the Edit menu, select Notification Devices.
- **Step 3** On the Notification Devices page, select the display name of the correct notification device.
- **Step 4** On the Edit Notification Device page, confirm that the Enabled check box is checked.
- **Step 5** 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 Set to Trigger Notification

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.
Changing the Message Types That Trigger a Notification Device

**Step 1**  
In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, in the Search Results table, select the alias of the applicable user.

**Step 2**  
On the Edit User Basics page, on the Edit menu, select **Notification Devices**.

**Step 3**  
On the Notification Devices page, select the display name of the correct notification device.

**Step 4**  
On the Edit Notification Device page, under Notification Rule Events, verify the selected message types with the user.

Notification Number Incorrect or Access Code for an External Line 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 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 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.

Verifying 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**. On the Search Users page, in the Search Results table, select the alias of the applicable user.

**Step 2**  
On the Edit User Basics page, on the Edit menu, select **Notification Devices**.

**Step 3**  
On the Notification Devices page, select the display name of the correct notification device.

**Step 4**  
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).

Testing a Phone or Pager Notification Device

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.

1. Confirm that the notification device is on.

2. 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.

3. On Phone 1, dial the notification number set in Unity Connection for the device.

If the pager is activated or the phone rings, you have confirmed that Unity 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.

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

**Notification Device Phone System Assignment Incorrect (Phone and Pager Notification Devices Only)**

**Verifying Notification Device Phone System Assignment**

**SUMMARY STEPS**

1. In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, in the Search Results table, select the alias of the applicable user.
2. On the Edit User Basics page, on the Edit menu, select **Notification Devices**.
3. On the Notification Devices page, select the display name of the correct notification device.
4. On the Edit Notification Device page, under Phone Settings, note the phone system that is specified in the Phone System field.
5. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
6. 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.

**DETAILED STEPS**

**Step 1**  
In Cisco Unity Connection Administration, expand **Users**, then select **Users**. On the Search Users page, in the Search Results table, select the alias of the applicable user.

**Step 2**  
On the Edit User Basics page, on the Edit menu, select **Notification Devices**.

**Step 3**  
On the Notification Devices page, select the display name of the correct notification device.

**Step 4**  
On the Edit Notification Device page, under Phone Settings, note the phone system that is specified in the Phone System field.

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

**Step 6**  
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 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 helps you troubleshoot the problem. For detailed instructions on enabling and collecting diagnostic traces, see the “Diagnostic Traces” chapter.

Common error codes and explanations for SMS problems are listed in the following table:
SMTP Message Notification 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 Unity Connection to send text message notifications using SMTP, your Unity 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 Unity 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 Unity 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” chapter.

HTML Notifications Not Working

If HTML notifications are not working, in Cisco Unity Connection Administration, check the HTML notification device under User > Edit > Notification Devices page is enabled and valid email address is added.

Also, verify that SMTP smart host is configured on Unity Connection Administration page and the Connection SMTP Server and Connection Notifier services are up and running.

HTML Summary Notification Not Working

If HTML Summary notifications are not working, verify that the correct template for Summary Notification is used under User > Edit > Notification Devices page on Connection Administration page. If the correct template is used, verify that valid <VOICE_MESSAGE_SUMMARY> tags are present inside the notification template with valid replaceable parameters are used inside the <VOICE_MESSAGE_SUMMARY> tags. For more information on missed call notification templates, see the Notifications chapter of System Administration Guide for Cisco Unity Connection Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html

Message Notifications Function Intermittently

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 Unity 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.


### Notification Devices Added in Unity Connection Administration 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.

Unity Connection Administration does not expose schedules for notification devices. From the Notification Device page for the user in Unity 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.


### Message Notification Received When No Unread Messages

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.

Message Notification Received When No Unread Messages
Troubleshooting Comet Notifications over SSL

Unable to Send Comet Notification over SSL

Make sure of the following if Unity Connection is unable to send comet notifications over SSL:

- User workstations are establishing connection on 7443 port.
- Firewall is not blocking the traffic on 7443 port.
- The show cuc jetty ssl status command is executed on both the primary and secondary nodes and the SSL mode is enabled.
- Connection Jetty service is restarted on both the primary and secondary servers.

For more information, see:

Unable to Send Comet Notification over SSL
CHAPTER 19

Troubleshooting a Cisco Unity Connection Cluster Configuration

• Troubleshooting a Cisco Unity Connection Cluster Configuration, on page 165

Troubleshooting a Cisco Unity Connection Cluster Configuration

One Server Stops Functioning and the Other Server is Not Handling Calls

When one Unity Connection server in a Unity 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.

Following are the tasks to troubleshoot when one server stops functioning and the other server is not handling 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.

2. Verify the voice messaging port assignments for the phone system integration. See the Verifying the Voice Messaging Ports Assignments for Phone System Integration.

3. For SCCP integrations, confirm that the voice messaging ports are registered with the Cisco Unified CM server. See the Confirming that Voice Messaging Ports are Registered (SCCP Integrations Only).

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 Diagnostic Traces for Troubleshooting, on page 1 section.

Note

Verifying the Status of the Voice Messaging Ports

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 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 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 Attain Primary Server Status

Use the troubleshooting information in this section if both servers in the 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 Unity 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.
Unity Connection Cluster Not Functioning Correctly

When a 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:

1. Confirm that the applicable services are running on the server with primary server status. See the Confirming that Applicable Services are Running on the Server with Primary Server Status.

2. Confirm that the applicable services are running on both servers. See the Confirming that Applicable Services are Running on Both Servers.

3. Use traces to troubleshoot the Unity Connection cluster. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Traces in Cisco Unity Connection Serviceability, on page 1.

Confirming that Applicable Services are Running on the Server with Primary Server Status

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Serviceability, on the Tools menu, select Service Management.</td>
</tr>
</tbody>
</table>
| 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 Applicable Services are Running on Both Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Serviceability, on the Tools menu, select Service Management.</td>
</tr>
</tbody>
</table>
| Step 2 | On the Control Center - Feature Services page, under Status Only Services, confirm that the Unity 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 11.0(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 Unity 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: |
Server Cannot be Added to the Unity Connection 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 Unity Connection cluster. See the following possible reasons why the Unity Connection cluster feature is not available:


- The number of servers in the Unity Connection cluster is the maximum that is supported. No more servers can be added to the Unity Connection cluster. For information on replacing Unity Connection servers in a Unity Connection cluster, see the “Replacing the Non Functional Server” section of “Maintaining Cisco Unity Connection Server” of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Cannot Access Alert Logs When the Publisher Server Stops Functioning

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.

Enabling the Subscriber Server to Access the Alert Logs When the Publisher Server Stops Functioning

1. On the publisher server, in Cisco Unity Connection Administration, expand System Settings, then select Service Parameters.
2. On the Service Parameters page, in the Server field, select the publisher server.
3. In the Service field, select Cisco AMC Service.
4. In the Failover Collector field, select the subscriber server.
5. Select Save.
Step 7 In the Server field, select the subscriber server and select Go.
Step 8 Under Performance and Monitoring, select Cisco AMC Service and select Restart.
Step 9 When prompted to confirm that you want to restart the service, select OK.
Enabling the Subscriber Server to Access the Alert Logs When the Publisher Server Stops Functioning
Troubleshooting Licensing

Troubleshooting Problems with Licenses

When a Cisco Unity Connection feature stops working, when Cisco Unity Connection Administration displays an alert concerning a license violation, or when Unity Connection stops functioning every 24 hours, use the following task list to determine whether the cause is a license violation. Following are the tasks to confirm that Unity Connection is not in license violation state:

1. Check if there are unused licensed seats for the applicable Unity Connection feature. To view the licenses that are used currently, see the "Managing Licenses in Cisco Unity Connection" chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html. To view the unused licenses on the ELM server, see the "Dashboard view" section of the ELM user guide.

2. Check if Unity Connection is not running in "Expire" mode.

3. Check if you need to add a licensed feature when Unity Connection is running in "Expire" mode.

Licensing Problems

The following section covers different licensing problems that may occur in Unity Connection and their solutions.

License Violation Status Appears on Cisco Unity Connection Administration

If Unity Connection is registered with the ELM server and the license violation status is displayed on the Cisco Unity Connection Administration, do the following:

• Confirm that a valid license file for the 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 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, check the network connectivity of the publisher server with the ELM 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, check the network connectivity of the subscriber server with the publisher server.

Unity Connection Not Answering Calls

If the Unity Connection server is not answering calls, make sure that the license status of the server is not “Expire”. If the license status is “Expire”, install the required licenses to change the license to “Compliance”.

Unity Connection Not Answering Calls After License Status Changes from “Expire” to “Compliance”

If Unity 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 Unity Connection, confirm whether the Unity Connection is configured with the ELM server and the required licenses for SpeechView are installed on the server.
CHAPTER 21

Troubleshooting Voice Recognition

- Troubleshooting Voice Recognition, on page 173

Troubleshooting Voice Recognition

Users Hear the Phone Keypad Conversation Instead of Voice-Recognition Conversation

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 yes, do the following:
   
   Confirm that the class of service (COS) is configured to enable voice recognition. On the Edit Class of Service page, under Licensed Features, check the Allow Access to Advanced Features check box and then check the Allow Users to Use Voice Recognition check box.
   
   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 yes, do the following:
   
   Confirm that the affected user is associated with the correct class of service.
   
   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, on page 174.

   1. Is the correct codec being used?

   Voice recognition does not work if the Unity 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 need to use the standard touchtones for the duration of this call,” do the following:

1. Confirm that the Connection Voice Recognizer service is running on the Tools > Service Management page in Cisco Unity Connection Serviceability.


2. Check the 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 Unity Connection server.

3. Check for errors generated by the Unity 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_NSServer_*.uc.


Voice Commands Recognized But Names Not Recognized

When administrators add or change names on the 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 Unity Connection automatically updates the name grammars.

• Make sure the Unity Connection Voice Recognition Transport service is running on the Tools > Service Management page in Cisco Unity Connection Serviceability.

• 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 different 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.)

Voice Commands Not Recognized

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 Unity 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.
   - If the user is having a problem with a single command, see the “Voice Commands” section in the “Phone Menus and Voice Commands” chapter of the User Guide for the Cisco Unity Connection Phone Interface (Release 11.x) for a list of preferred voice commands. (The guide is available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user/guide/phone/b_11xcucuphone.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.
   - If the user is having a problem with Unity Connection taking unintended actions without prompting for confirmation, or if Unity Connection is prompting for confirmation too frequently, check the Voice Recognition Confirmation Confidence Threshold setting. See the Checking the Voice Recognition Confirmation Confidence Setting.

2. Try to reproduce the problem while running the Remote Port Status Monitor to determine which voice commands as per Unity Connection are being uttered. See the Using the Remote Port Status Monitor.

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.

4. Enable diagnostic traces and try to reproduce the problem. See the Using Diagnostic Traces for Voice Recognition.
Checking the Voice Recognition Confirmation Confidence Setting

You can use the Voice Recognition Confirmation Confidence Threshold setting to specify how frequently Unity Connection should prompt 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 Threshold 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

This section covers the diagnostic tools that help you troubleshoot voice-recognition problems.

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 Using Diagnostic Traces for Troubleshooting, on page 1 section.

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 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), 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 MiIO level 25 micro trace for ASR and MRCP.)

You can access the utterance files using the Real-Time Monitoring Tool (RTMT).

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.

Enabling and Viewing Utterance Capture Traces 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 Unity 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 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 > Unity Connection Voice Recognition Transport folder.
Step 14 In the Unity 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In a web browser, go to the Cisco Unity Tools website at <a href="http://www.ciscounitytools.com">http://www.ciscounitytools.com</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Tool Update Log section, select <strong>Port Status Monitor</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Cisco Unified Communication Tools page for the Port Status Monitor, select <strong>Download Now</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Follow the on-screen instructions to download the Remote Port Status Monitor tool.</td>
</tr>
</tbody>
</table>

---

**To Configure 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 and select Save. |

**Note**   You can enter up to 70 IP addresses. Each IP address must be separated from the following IP address by a comma.
Troubleshooting the Conversation

Custom Keypad Mapping Not Taking Effect

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

Changing the Conversation Style for a Single User

1. In Cisco Unity Connection Administration, expand Users and then select Users. On the Search Users page, select the alias of the user.
2. On the Edit menu, select Phone Menu.
3. In the Touchtone Conversation Menu Style list, select the applicable Custom Keypad Mapping and select Save.

Specifying a Custom Keypad Mapping Conversation for Multiple User Accounts at Once

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.
2. On the Edit menu, select Phone Menu.
3. In the Touchtone Conversation Menu Style list, select the applicable Custom Keypad Mapping.
4. If applicable, set the Bulk Edit Task Scheduling fields to schedule the Bulk Edit operation for a later date and/or time and select Submit.
Long Pauses After Listening to Help Menu

After playing a Help menu, 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.

Determine the WAV File Played

To determine which WAV file is being played off from the hard disk, do the following procedures in the order given.

Downloading 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.

Configuring Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand System Settings > and 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 Port Status Monitor Output field, enter the IP addresses of your workstations and select Save.

Note You can enter up to 70 IP addresses, separated by commas.

Enabling 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 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 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.
Troubleshooting SAML SSO Access

Redirection to IdP fails

When the end users attempt to log into a SAML-enabled web application using a Cisco Unity Connection supported web browser, they are not redirected to their configured Identity Provider (IdP) to enter the authentication details. Check if the following conditions are met:

- The Identity Provider (IdP) is up and running.
- The correct IdP metadata file (idp.xml) is uploaded to Unity Connection.
- Verify if the server and the IdP are part of the same circle of trust.

IdP authentication fails

If the end user is not getting authenticated by the IdP, check if the following conditions are met:

- The LDAP directory is mapped to the IdP.
- The user is added to the LDAP directory. If the problem still exists, then check the NTP servers associated with Unity Connection and Identity Provider. Make sure that the time on NTP servers associated to both these servers are in synchronization.
- The LDAP account is active.
- The User Id and password are correct.

Redirection to Unity Connection fails

Even after getting authenticated by the IdP, if the user is not redirected to SAML SSO enabled web applications, check the following:
• The clocks of the Unity Connection and the IdP are synchronized. See the "NTP Servers" section in Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/os_administration/b_11xcucosagx.html

• The mandatory attribute uid is configured on the IdP.
• The correct Unity Connection server metadata file is uploaded to the IdP.
• The user has the required privileges.

Run Test Fails

When the Run Test fails on Unity Connection, refer the corrective actions that are outlined in Redirection to IdP fails, IdP authentication fails and Redirection to Unity Connection fails.

Mismatch in SAML Status on Publisher and Subscriber Servers

When there is a mismatch of SAML status on publisher and subscriber servers in Unity Connection, do the following:

• Check if IdP metadata is correct on Subscriber server, if not then select the option Re-import Meta Data from SAML Single Sign-On web page.
• If problem still exists, then select the option Fix All Disabled Servers.

Note

There is no option to re-import meta data for Publisher server in case of Unity Connection cluster.

Problem in Accessing Web Application on Unity Connection

When a user is not able to access the web applications on Unity Connection using SAML SSO feature and encounters the given error:

Error
<ADFS server>

There was a problem accessing the site. Try to browse to the site again. If the problem persists, contact the administrator of this site and provide the reference number to identify the problem.

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

1. Confirm that the Service Provider metadata (SPMetadata<hostname of Unity Connection>.xml) is not missing on Identity Provider. Try uploading the Service Provider metadata of the Unity Connection via Import or URL option.

2. After importing the sp.xml successfully, add the following two claim rules:

   • Send LDAP Attributes as Claims: Select LDAP attribute as SAM-Account-Name and add Outgoing Claim type corresponding to this as uid.
   • Send Claims using a Custom Rule: Under the Custom Rule description, write the following claim:
c: Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname")
  -> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
    Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
    Properties{"http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"
      = "http://<ADFS_FQDN>/adfs/com/adfs/service/trust",
    Properties{"http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
      = "<UC_Node_FQDN>");

Save these two claim rules successfully to ensure that Identity Provider used in SAML SSO feature is configured
well. (In the above problem description, we have considered ADFS as Identity Provider for
SAML SSO. You may choose any of the supported Identity Provider instead.)

1. The Unity Connection server entry on Identity Provider server must not be disabled.
2. There should be any errors upon accessing the Service Provider metadata (SPMetadata<hostname of Unity
Connection>.xml) as a corrupted SP metadata file never allows a user to gain single sign-on access to
web applications.

Encryption Error Upon User Login to Unity Connection

When a user tries to login to a web application on Unity Connection and encounters the following
exception error:
Error 500 with Exception
Unable to decrypt secret key

Use the following task list to determine the source of the problem and correct it:
1. Confirm that the SAML SSO feature is enabled on Unity Connection.
2. Under the Identity Provider server Relying party trust page, select Edit Claim Rule and then select
Encryption tab. Remove the encryption from that location and the issue gets fixed.

Unable to Upload Subscriber SP Metadata on ADFS in Cluster

When a user tries to upload the subscriber’ SP metadata on ADFS server in a cluster and it fails, the user must
try the following steps:
1. Update roll 3 on ADFS 2.0 with hotfix. (http://support.microsoft.com/kb/2790338).
2. Start Windows powershell and run the command:
   cd "$env:programfiles\active directory federation services 2.0\sql"
   Add-PSSnapin microsoft.adfs.powershell
   \PostReleaseSchemaChanges.ps1

Note: If you get following error at powershell
script cannot be loaded because the execution of scripts is disabled on this system
SAML Exception Time Synchronization Error

When a user tries to configure SAML SSO feature on Unity Connection and encounters the following error related to time mismatch:

SAML Exception issue: SAML2Exception
The time in SubjectConfirrationData is invalid

Use the following task list to determine the source of the problem and correct it:
1. Make sure that the clocks of Identity Provider (like ADFS) and Unity Connection are in synchronization with each other.
2. If the problem still exists, then check the NTP servers associated with Unity Connection and Identity Provider. Make sure that the time on NTP servers associated to both these servers are in synchronization.

Incorrect status of SAML SSO on Two Servers in a Unity Connection Cluster

When the status of SAML SSO feature is different on the two servers in a Unity Connection cluster, do the following:

• If SAML SSO status is disabled on subscriber server and enabled on publisher server, login to Cisco Unity Connection Administration on subscriber server, and select the option “Fix All disabled servers”.
• If we disable the SAML SSO feature on subscriber server when the publisher server is not reachable, a user needs to explicitly disable the SAML SSO feature from publisher server and vice versa. You may also be required to reboot the server if the issue still persists.
• In case of publisher rebuild, administrator needs to explicitly update the IdP metadata file on the publisher server of cluster.

Troubleshooting Cross Origin Resource Sharing

When a third party browser application makes CORS request from a different origin to get the status of SAML Single Sign On by calling the http://<hostname>/ssosp/ws/public/singleSignOnAPI, the user may get the “Domain not Allowed” error message. To resolve this issue:

• Verify if the domain name is configured properly into the trace file.
• Check if the API method type is configured correctly.
• Verify if the <Hostname> is mentioned correctly in the API.

Diagnostics Traces for Problems with SAML SSO Access

You can enable the Unity Connection trace levels to detect and study any issues related to SAML SSO feature. The traces are turned on from command line access(CLI) to the system server.

The given command turn on the traces for SAML SSO:
admin: set samltrace level <trace-level>

The traces defined are:
- Debug
- Info
- Warning
- Error
- Fatal

The traces are collected in the following location on Unity Connection:
/var/log/active/tomcat/logs/ssosp
Troubleshooting Fax

Problems with Fax Delivery to Users

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.

Following are the tasks to troubleshoot 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 Diagnostic Traces for Troubleshooting, on page 1 section.

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 Diagnostic Traces for Troubleshooting, on page 1 section.

3. Confirm that the SMTP server configuration lists the IP address of the Cisco Fax Server and allows a Unity Connection. See the Confirming that SMTP Server Configuration is Correct.

4. Check for the fax in the POP3 mailbox by connecting an email client to the POP3 mailbox.

5. In the RightFax Email Gateway, confirm that the POP3 mailbox name and password are correct. See the Confirming that POP3 Mailbox Name and Password are Correct.

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 Unity Connection. See the Confirming Fax is Delivered to Unity Connection.

Note

The email client must be configured to leave messages in the POP3 mailbox.
Confirming that SMTP Server Configuration is Correct

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In Cisco Unity Connection Administration, expand System Settings &gt; and select SMTP Configuration &gt; Server.</td>
</tr>
<tr>
<td>2</td>
<td>On the SMTP Server Configuration page, on the Edit menu, select Search IP Address Access List.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Check the Allow Connections check box for the IP address of the Cisco Fax Server, if it is not already checked and select Save.</td>
</tr>
</tbody>
</table>

Confirming that POP3 Mailbox Name and Password are Correct

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the Windows Start menu, select Control Panel &gt; RightFax Email Gateway.</td>
</tr>
<tr>
<td>2</td>
<td>In the Email Configuration window, select the General tab.</td>
</tr>
<tr>
<td>3</td>
<td>In the POP3 Mailbox Name field, confirm that the entry matches the SMTP address for the Cisco Fax Server on the System Settings &gt; Fax Server &gt; Edit Fax Server Configuration page in Cisco Unity Connection Administration.</td>
</tr>
<tr>
<td>4</td>
<td>In the Mailbox Password field, confirm that the password is correct.</td>
</tr>
<tr>
<td>5</td>
<td>In the Email Deliver Direction field, confirm that Both is selected and select OK.</td>
</tr>
</tbody>
</table>

Confirming Fax is Delivered to Unity Connection

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the Windows Start menu, select All Programs &gt; RightFax FaxUtil.</td>
</tr>
<tr>
<td>2</td>
<td>In the RightFax FaxUtil window, in the left pane, select the user who sends the test fax.</td>
</tr>
<tr>
<td>3</td>
<td>On the Fax menu, select New.</td>
</tr>
<tr>
<td>4</td>
<td>In the Fax Information dialog box, select the Main tab.</td>
</tr>
<tr>
<td>5</td>
<td>Under the Name field, select the drop-down arrow and select Email Address.</td>
</tr>
<tr>
<td>6</td>
<td>In the Email Address field, enter the email address of the user who has the fax delivery problem.</td>
</tr>
<tr>
<td>7</td>
<td>Select Save.</td>
</tr>
<tr>
<td>8</td>
<td>In the right pane, note the status of the test fax as it is being sent.</td>
</tr>
</tbody>
</table>

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

Problems with Fax Delivery to a Fax Machine

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.

Following are the tasks to troubleshoot fax delivery issues in a fax machine:
1. Determine the status of the fax that was sent to a fax machine. See the Determining the Status of a Fax Delivered to a Fax Machine.

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 POP3 Mailbox Name and Password are Correct.

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 Unity Connection. See the Confirming that SMTP Server Configuration is Correct.

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 Diagnostic Traces for Troubleshooting, on page 1 section.

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 Diagnostic Traces for Troubleshooting, on page 1 section.

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 Faxable File Types List is Correct.

---

**Determining the Status of a Fax Delivered to a Fax Machine**

**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 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 and select **OK**.

---

**Confirming that SMTP Server Configuration is Correct**

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

Confirm that fax notification from Unity Connection is enabled for the user.

Confirming that Fax Notification is Enabled for the User

Step 1  In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, select the alias of the user.
Step 2  On the Edit menu, select Notification Devices.
Step 3  On the Notification Devices page, select the name of the applicable notification device.
Step 4  On the Edit Notification Device page, under Notification Rule Events, check the Fax Messages check box and select Save.

Problems with Fax Receipts

This section covers the troubleshooting steps of some fax receipt related problems.

Fax Receipts Not Delivered

Verifying 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, Unity 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, Unity Connection notifies the user of the successful fax.

Step 9 Select OK.

---

**Verifying 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 **Verifying Prefixes for Delivery Receipts and Nondelivery Receipts on the Cisco Fax Server**.

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 **Verifying Prefixes for Delivery Receipts and Nondelivery Receipts on the Cisco Fax Server**.

Step 4 Select **Save**.
User Mailbox is Filled with Fax Notifications

Disabling 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

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 Diagnostic Traces for Troubleshooting, on page 1 section.

- Confirm that the faxable file types include the file types that you sent to the fax machine for printing. See the Confirming that Faxable File Types List is Correct.

Confirming that 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**.
Troubleshooting Reports

Overview

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

1. Confirm that the Unity Connection Reports Data Harvester service is running. See the Confirming Connection Reports Data Harvester Service is Running.

2. Adjust the report data collection cycle. See the Adjusting Report Data Collection Cycle.

3. Use traces to troubleshoot reports. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Using Diagnostic Traces for Troubleshooting, on page 1 section.


Confirming Connection Reports Data Harvester Service is Running

Step 1  In Cisco Unity Connection Serviceability, expand 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 Report Data Collection Cycle**

**Step 1**  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.

**Step 2**  In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Reports**.

**Step 3**  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 4**  Select **Save**.
Troubleshooting Cisco Personal Communications Assistant (PCA)

- Overview, on page 195
- Users cannot Access Cisco PCA Pages, on page 196
- Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages, on page 196
- Users cannot Access Unity Connection Web Tools from Cisco PCA, on page 197
- Users cannot Save Changes on Pages in Cisco PCA, on page 197
- Cisco PCA Error Messages, on page 197
- Missing Text on the Menu Bar (Microsoft Windows Only), on page 200
- Verifying if Tomcat Service is Running, on page 201

Overview

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 Unity Connection. The Unity 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 Unity Connection server during installation.

Following are the tasks to troubleshoot problems with Cisco Personal Communications Assistant:

- If there is an error message associated with the problem, review the Cisco PCA Error Messages.

- Review the Users cannot Access Cisco PCA Pages 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, on page 29 chapter for the applicable troubleshooting procedures.

- If the problem is that Media Master does not show up correctly or at all, see the Troubleshooting MediaMaster, on page 235 chapter.

- If the problem is that the menu bar does not display any text, see the Missing Text on the Menu Bar (Microsoft Windows Only).

- Confirm that the Tomcat service is running. See the Verifying if Tomcat Service is Running.
Users cannot Access Cisco PCA Pages

Users cannot Access Cisco PCA Pages

Users use the Cisco Personal Communications Assistant (PCA) website to access the Messaging Assistant, and the 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 11.x. The guide is available at [https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwxs.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwxs.html).


In addition, users can access the Web Inbox URL, and link to the Messaging Assistant and Personal Call Transfer Rules pages from there. The Web Inbox URL is http://<Unity Connection server>/inbox.

Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages

If you use the self-signed certificate generated during installation to provide an SSL Unity 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 Unity Connection, some email clients supported for use with Unity Connection display SSL security messages.

Although users can still access Unity 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 Adding 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 does not see the alert again.
Adding the SSL Certificate to the Trusted Root Store on User Workstations

Step 1  From the OS Administration application on the 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 using tools in the browser or IMAP client, as applicable.

Users cannot Access Unity Connection Web Tools from Cisco PCA

When users can access the Cisco Personal Communications Assistant (PCA), but cannot access the Messaging Assistant, or the 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 Cisco Personal Communications Assistant (PCA) chapter for Web Inbox troubleshooting information.

  • In order to access the 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 Cisco PCA

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 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.

Cisco PCA Error Messages

In addition to browser error messages (such as “File not found” or “Unauthorized access”), users may see Cisco PCA-specific error messages, Java plugin error messages, and Tomcat error messages when 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:

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser error messages</td>
<td>Browser error messages may indicate that the Cisco PCA failed to install, the user does not have network access to the 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).</td>
</tr>
<tr>
<td>Cisco PCA-specific error messages</td>
<td>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.</td>
</tr>
<tr>
<td>Java Plugin error messages</td>
<td>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.</td>
</tr>
<tr>
<td>Tomcat error messages</td>
<td>Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the 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.</td>
</tr>
</tbody>
</table>

**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.
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 using the `utilscucresetpassword` 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.)


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.ClassFormatException: <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 if Tomcat Service is Running](#).

**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 Unity 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: “Application Blocked by Security Settings. Your security settings have blocked a self-signed application from running"

The users receive an error message: “Application Blocked by Security Settings. Your security settings have blocked a self-signed application from running”, under the following conditions:

- While uploading an existing .wav file or saving a new recorded message as a voice name or
- While uploading an existing .wav file or saving a new recorded message as a greeting.

Using Media Master bar with Java version 7 latest update on IE as the web browser.

To correct the problem, follow the given steps:
1. Select Security tab of Java Control panel.
2. Select Add in the Exception Site List window.
3. Type the URL into the empty field that is provided under Location.
4. Continue to select Add and enter URLs until your list is complete. Select OK to save the URLs that you entered.
5. If you select Cancel, the URLs are not saved.

Error Message “Access denied” When Trying to Play Recordings through Media Master 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 (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.

Re-Registering 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 if Tomcat Service is Running

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 using either Real-Time Monitoring Tool (RTMT) or the Command Line Interface (CLI). Do the applicable procedure:
   • Confirming That the Tomcat Service Is Running Using Real-Time Monitoring Tool (RTMT)
   • Confirming That the Tomcat Service Is Running Using the Command Line Interface (CLI)

2. If necessary, restart the Tomcat service using the Command Line Interface (CLI). See the Restarting the Tomcat Service Using the Command Line Interface (CLI).

Confirming That the Tomcat Service Is Running Using Real-Time Monitoring Tool (RTMT)

Step 1 Launch Real-Time Monitoring Tool (RTMT).


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.

Confirming That the Tomcat Service Is Running Using the Command Line Interface (CLI)

Step 1 Use the Command Line Interface (CLI) command `utils service list` to list all of the services.


Step 2 Scan the CLI output for the Cisco Tomcat service and confirm that its status is Started.
To restart the Cisco Tomcat service, use the CLI command `utils service restart Cisco Tomcat`.

Troubleshooting Personal Call Transfer Rules

Personal Call Transfer Rules Settings Unavailable

If a user does not hear the Personal Call Transfer Rules Settings menu in the phone interface or if a user cannot see the Cisco Unity 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” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Determining 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

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**

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.

**Enabling 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**

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

- **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 Not Applied Correctly.

- **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 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 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.

• 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.

Turning On Personal Call Transfer Rules for an Individual User

Step 1

In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, select the alias of the user for whom you want to turn on personal call transfer rules.
Rules Based on a Meeting Condition 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, confirm that all settings are correct.

- Confirm that the applicable service is configured as an Unified Messaging 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 and verify settings.


- Confirm that the Exchange-server and Unity 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.

- To permanently change the interval at which Unity Connection caches calendar information, see the Changing the Interval at Which Unity Connection Caches Calendar Information.

Forcing an Immediate Caching of Calendar Appointments

Do the following procedure to force Cisco Unity Connection to immediately cache calendar information.

---

**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 Unity Connection Caches Calendar Information

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

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 Unity 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 Unity 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 Unity 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 Unity Connection waits between polling cycles when it caches upcoming Outlook calendar data for calendar users who must have their calendar caches updated more frequently.

Problems with Transfer All Rule

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 Using Personal Call Transfer Rules

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 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 Unity Connection Unavailable](#).

• **Users notice inconsistencies in how calls are placed through Cisco Unity Connection or dialed directly**—See the [Inconsistent Behavior in Calls Placed through Unity Connection and Calls Placed Directly to a User Phone](#).

• **Calls loop during rule processing**—See the [Call Looping During Rule Processing](#).

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

---

**Note**
The information in this section is not applicable to Cisco Business Edition.

---

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**

2. Check to see if the publisher Cisco Unified CM server is shut down or if there are network connectivity issues between 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, Unity Connection cannot change the Call Forward All (CFA) setting for the phone.
The option to forward all calls to Unity 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 Unity Connection and Calls Placed Directly to a User Phone**

Callers may notice inconsistent behavior when calling a user through the 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 Unity 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 Unity Connection are forwarded back to Unity 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 Unity Connection to detect and terminate call looping conditions so that calls proceed correctly.

- In the 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 Unity Connection forwarding calls to the mobile phone of the user, and the mobile phone forwarding the calls back to Unity Connection. When the Loop Detection setting is enabled, Unity 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 Unity 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 Unity Connection destinations to 3 rings allows Unity Connection to maintain control of the call. The supervised transfer initiated by Unity 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

You can use traces to troubleshoot problems with personal call transfer rules. For detailed instructions on enabling and collecting diagnostic traces, see the Using Diagnostic Traces for Troubleshooting, on page 1 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

**SUMMARY STEPS**

1. Launch Real-Time Monitoring Tool (RTMT).
2. In RTMT, on the System menu, select **Performance > Open Performance Monitoring**.
3. Expand the Unity Connection server.
4. Expand **CUC Personal Call Transfer Rules**.
5. Select the applicable counters:

**DETAILED STEPS**

**Step 1**
Launch Real-Time Monitoring Tool (RTMT).

**Note**
Step 2  In RTMT, on the System menu, select **Performance > Open Performance Monitoring**.

Step 3  Expand the Unity 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.
Troubleshooting Web Inbox

Introduction

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 Unity Connection voice messages using a web browser. It is installed on the Unity Connection server during installation.

Following are the tasks to troubleshoot problems with Web Inbox:

- If there is an error message associated with the problem, review the Web Inbox Error Messages.
- Review the Adobe Flash Player Settings Dialog Box Unresponsive (Mac OS X with Firefox Only) 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 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 Unresponsive (Mac OS X with Firefox Only).
- If the problem is that no messages are displayed in the Web Inbox, see the Messages Not Displayed in Web Inbox.
- If the problem is that users do not see any sent items in the Sent Folder, see the Sent Messages Not Displayed in Web Inbox.
- Confirm that the Tomcat service is running. See the Verifying that Tomcat Service is Running.
- 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.

If you cannot resolve the problem and plan to report the problem to Cisco TAC, you are asked to provide information about your system and about the problem.
Web Inbox Error Messages

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:

<table>
<thead>
<tr>
<th>Error Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser error messages</td>
<td>Browser error messages may indicate that the Web Inbox failed to install, the user does not have network access to the 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).</td>
</tr>
<tr>
<td>Web Inbox-specific error messages</td>
<td>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.</td>
</tr>
<tr>
<td>Quicktime Plugin error messages</td>
<td>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.</td>
</tr>
<tr>
<td>Tomcat error messages</td>
<td>Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the 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.</td>
</tr>
</tbody>
</table>

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

**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.


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 Tomcat Service is Running.

**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 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 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 Unity Connection account.

**Error Message: “Error While Uploading Message to Server”**

If a user sign in to a Web Inbox using Mozilla Firefox and sends a voice message by uploading the .wav file, an error message “Error while uploading message to server” gets displayed on the Web Inbox, However, the recipient still receives the voice message.

**Removing the Error Message Displayed on the Web Inbox**

**SUMMARY STEPS**

1. Uninstall the Mozilla Firefox browser.
2. Clear your data from Mozilla Firefox:
3. Reinstall the Mozilla Firefox browser again.

**DETAILED STEPS**

**Step 1** Uninstall the Mozilla Firefox browser.

**Note** Uninstalling the Firefox does not remove any user data, such as cache or history. To completely remove the user data, you must manually delete the Firefox folder that contains the user profile.
Step 2 Clear your data from Mozilla Firefox:
   a) Select the Windows Start button and enter %APPDATA% in the search field.
   b) Press Enter to open the hidden Roaming folder. The Mozilla folder gets displayed.
   c) Open the Mozilla folder and delete the Firefox folder to manually delete the user profile.

Step 3 Reinstall the Mozilla Firefox browser again.

Error Message: "HTML5 audio compatible browser or QuickTime Plug-in not found. Select Phone option to play the message. Install Quick time plugin or open web inbox into firefox"

If a user signs into a Web Inbox using Internet Explorer 11 Mozilla Firefox and sends a voice message by uploading the .wav file, an error message "Error while uploading message to server" gets displayed on the Web Inbox. However, the recipient still receives the voice message.

Send Option is Disabled on MAC Operating System

On MAC operating system, if the Send option on Safari is not working after uploading voice message, make sure that the most recent version of Flash Player is installed on your machine. If the latest version of Flash Player is installed on your system but still the Send option is not working, do the following to resolve the issue:

Step 1 Navigate to Safari > Preferences and select Security tab.
Step 2 Check the Allow Plug-ins check box on the Security tab.
Step 3 Click Website Settings.
Step 4 In Configured Websites, select Allow Always for the Unity Connection server.

Adobe Flash Player Settings Dialog Box 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.
Changing 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 Not Displayed in 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 Not Displayed in 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 Tomcat Service is Running

Do the following tasks to confirm that the Tomcat service is running in Unity Connection and if necessary, to restart the Tomcat service:

1. **Confirming that the Tomcat Service is Running Using Real-Time Monitoring Tool (RTMT)**
   - Confirm that the Tomcat service is running using either Real-Time Monitoring Tool (RTMT) or the Command Line Interface (CLI). Do the applicable procedure:
     - **Confirming that the Tomcat Service is Running Using Real-Time Monitoring Tool (RTMT)**
     - **Confirming that the Tomcat Service is Running Using the Command Line Interface (CLI)**

2. If necessary, restart the Tomcat service using the Command Line Interface (CLI). See the **Restarting the Tomcat Service Using the Command Line Interface (CLI)**.

**Confirming that the Tomcat Service is Running Using Real-Time Monitoring Tool (RTMT)**

**Step 1**
Launch Real-Time Monitoring Tool (RTMT).

**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.

---

### Confirming that the Tomcat Service is Running Using the Command Line Interface (CLI)

**Step 1** Use the Command Line Interface (CLI) command `utils service list` to list all of the services.


**Step 2** Scan the CLI output for the Cisco Tomcat service and confirm that its status is **Started**.

---

### Restarting the Tomcat Service Using the Command Line Interface (CLI)

To restart the Cisco Tomcat service, use the CLI command `utils service restart Cisco Tomcat`.


---

### 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.
Troubleshooting the HTML Notifications

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 Mini Web Inbox. 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, see the "Configuring User Templates" section of the "User Attributes" chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html


It is recommended, that the Mini Web Inbox must always be opened from the notification email as it requires certain URL parameters.

- HTML Notifications Not Received By the Users, on page 219
- Images Not Displayed on Microsoft Outlook, on page 220
- Images Not Displayed on IBM Lotus Notes, on page 221
- Hyperlinks Not Visible in the Email Notification, on page 221
- Unable to Launch Mini Web Inbox, on page 221
- Unable to View the Updated Mini Web Inbox Interface in Internet Explorer, on page 221
- Unable to Play and Record Voice Messages on Computer Using Mini Web Inbox, on page 222

HTML Notifications 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, see the "Integrated Messaging" section of the "Messaging" chapter of the System Administration Guide for System Administration Guide for Cisco Unity Connection Release 11.x,
• Ping the smart host from Unity Connection server. If the ping fails, there is a possibility that network
Unity Connection is not functional and you must restore the network Unity Connection.
• Confirm that the 'Unity 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, see the "Notifications" chapter of the System Administration Guide for Cisco Unity
11x/administration/guide/b_cucsag.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, see the "Notifications" chapter of the

Images 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, see the "Configuring Microsoft Outlook to Display Images in
an HTML Message Notification" section of the "Configuring an Email Account to Access Cisco Unity
Connection 10.x Voice Messages" chapter of the User Workstation Setup Guide for Cisco Unity
11x/user_setup/guide/b_11xcucuwsx.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 Unity Connection does 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 Unity Connection credentials then no image is displayed in the email notification. You must restart
the Outlook to enter the Unity 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, see 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 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 Unity Connection Server with Internet Explorer by copying the link of the images
and manually opening it on 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 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, see the "Configuring the Authentication Mode" section of the "Configuring an Email Account to Access Cisco Unity Connection 10.x Voice Messages" chapter of the User Workstation Setup Guide for Cisco Unity Connection, Release 10.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwsx.html

Hyperlinks 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.


Unable to Launch Mini Web Inbox

If the user is unable to launch the 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 Unity Connection Mini Web Inbox is not deleted.
• Confirm that the user is logged in with the valid username.

Unable to View the Updated Mini Web Inbox Interface in Internet Explorer

To View the Updated Interface of Unity 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 Mini Web Inbox

If the user is unable to play and record voice messages on computer using Unity 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, see the "Configuring Notification Devices" section of the "Notifications" chapter of the System Administration Guide for Cisco Unity Connection, Release 10.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html
- Confirm that the callback number is configured.
- Confirm that the end user answers the phone.
CHAPTER 30

Troubleshooting Custom Roles

This section covers the problems that you might face while creating, updating, deleting or assigning custom roles to users.

- Troubleshooting Custom Roles, on page 223

Troubleshooting Custom Roles

This section covers the problems that you might face while creating, updating, deleting or assigning custom roles to users.

Unable to Configure Custom Role

While creating, updating or deleting a custom role, if you receive the "Not Authorised" error message, confirm that you are logged in as a system administrator. Only a user with system administrator role can create, update or delete custom roles.

Getting "Not Authorized" Error Message on Role Assignment or Unassignment

If you are not able to assign or unassign a custom role to any user, check the following:

1. Confirm that you are not trying to assign any of the system roles to the user. A system role can be assigned to users only by the system administrator.
2. Confirm that you have a role with Manage Users: Assign/Unassign Roles privilege. Do the following steps to confirm the same:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unity Connection Administration page, go to Users and select your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Go to Edit &gt; Roles and note the role in the Assigned Role field.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Go to System Settings &gt; Roles &gt; Custom Roles page and on the Search Custom Role page select the role assigned to you.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Edit Custom Role page check if the check box for the &quot;Manage Users: Assign/Unassign Roles&quot; privilege is checked. If the checkbox is not checked that means you do not have the privilege to assign or unassign roles.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Contact the system administrator to assign the privilege to the role assigned to you.</td>
</tr>
</tbody>
</table>
Getting "Not Authorized" Error on Cisco Unity Connection Administration Pages

After logging in to Cisco Unity Connection Administration page, if you are getting "Not Authorized" error on every page, contact the system administrator to check that you have a role with "Read Access To System Configuration Data - Read Access" privilege.

Troubleshooting Tenant Partitioning

Troubleshooting Problems While Configuring Tenant Partitioning
This section covers the problems that you might face while configuring tenant partitioning.

Getting Error Message "COS is referenced by at least one user or user template" while Deleting a Tenant
While deleting a tenant you may get this error message "COS is referenced by at least one user or user template". This error may occur for any other objects that are associated with the tenant. This error occurs if the objects mapped to a tenant like class of service are associated with users belonging to other tenants.

- Troubleshooting Issues while Deleting Tenant, on page 225
- Users of One Tenant are Able to Send Messages to Users of Other Tenants, on page 226
- Able to Hear the Opening Greeting Without being Asked for the PIN, on page 226
- Getting Option to Select Users from Other Partitions in Directory Result, on page 227
- Tenant Creation Fails with an Error Message "Non-Tenant users exist on Unity Connection", on page 227
- Troubleshooting Problems While Integrating with Call Manager, on page 228
- Troubleshooting Problems with Migration, on page 229

Troubleshooting Issues while Deleting Tenant

**Step 1** Get object IDs of the class of service objects associated with the tenant using the URI:
https://<connection-server>/vmrest/tenants/<TenantObjectId>/coses

Get the list of user templates associated with the class of service object ID using the URI:
https://<connection-server>/vmrest/usertemplates?query=(CosObjectId%20is%20<CosObjectId>)

Here, replace <CosObjectId> with the COS ObjectId that belongs to the tenant.

To get the list of user templates that belongs to the tenant, use the URI below:
https://<connection-server>/vmrest/usertemplates?query=(CosObjectId%20is%20<CosObjectId>%20&PartitionObjectId%20is%20<PartitionObjectId>)

**Step 2** Comparing results of the GET operations would provide list of user templates that are associated with the tenant's class of service but are not a part of tenant's partition. You can correct this by changing the class of service association for these user templates.

**Step 3** Get the list of users associated with the class of service Object ID using the URI:
Users of One Tenant are Able to Send Messages to Users of Other Tenants

If the users of one tenant are able to send messages to users of other tenants through the Web Inbox, touchtone, or voice recognition conversation, do the following:

1. Check the tenant's search space as it may contain partition(s) belonging to other tenants.
2. Run an HTTP GET request on the URI below to get Search Space Object ID for the tenant:
   https://<connection-server>/vmrest/searchspacesmembers?query=(PartitionObjectId%20is%20<TenantPartitionObjectId>)
3. Run an HTTP GET request on the URI below to get the object ID for partitions belonging to the tenant's search space:
   https://<connection-server>/vmrest/searchspacesmembers?query=(SearchSpaceObjectId%20is%20<TenantSearchSpaceObjectId>)
4. Correct this by changing the association.

Able to Hear the Opening Greeting Without being Asked for the PIN

If you are able to hear the opening greeting without being asked for the PIN, do the following:

1. Open Port Status Monitor and dial the pilot number.
2. On Port Status Monitor and check if the calls are going directly to the opening greeting.
3. To check this, get the list of routing rules for the tenant by sending a GET request to the URI and check the value for the Rule Index field:
   GET
   https://<connection-server>/vmrest/routingrules?query=(SearchSpaceObjectId%20is%20<TenantSearchSpaceObjectId>)

To correct the routing rule order, see the CUPI APIs documentation for Routing Rules API.

http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Provisioning_Interface_%28CUPI%29_API_-_Routing_Rules
Getting Option to Select Users from Other Partitions in Directory Result

1. Check Search Scope for the directory handler that belongs to the tenant.
2. If the value of SearchScope field is set to zero then it means that the Search Scope is set to entire server. Set the search scope value to 6 to resolve the issue.
3. There is a possibility that the SearchScope field is set to search-space of some other tenant. Set the search scope to search space of respective tenant to resolve the issue.

Debugging Steps

1. Check Search Scope for the directory handler that belongs to the tenant. To do this, run the following HTTP GET request:

   https://<connection server>/vmrest/handlers/directoryhandlers?query=(PartitionObjectId%20is%20<TenantPartitionObjectId>)

   If the value of SearchScope field is set to zero then it means that the Search Scope is set to entire server. Set the search scope value to 6 to resolve the issue.

2. Enable Micro Traces for General Method returns and Parameter values(01), Data access(02), Named property access(03) level ConvSub logs and Named props access(11), CDL Access(12), MIU Access(13) and Search Space(04) level CDE logs from Cisco Unity Connection Serviceability.

3. For all the aliases that you hear over the call, there may be an entry in the diag_CuCsMgr_*.uc log files.

4. Search space can contain multiple partitions. To check if there are multiple partitions in search space, you can run the following HTTP GET request:
   1. Get the search space: GET

      https://<connection server>/vmrest/searchspaces/<searchspace-objectid>/searchspacemembers?query=(PartitionObjectId%20is%20<TenantPartitionObjectId>)

      From the above URI search space object ID of a tenant is obtained and it can be used to find the associated partitions with the URI below.

   2. To get the search space: GET

      https://<connection server>/vmrest/searchspaces/<searchspace-objectid>/searchspacemembers?query=(SearchSpaceObjectId%20is%20<SearchSpaceObjectId>)

5. Check if the search space selected in search scope of directory handler belongs to the same tenant or not. To do this, run the following HTTP GET request:

   https://<connection server>/vmrest/handlers/directoryhandlers/<directoryhandler-objectid>

   Check the search scope object ID, it should be same as that of the tenant.

Tenant Creation Fails with an Error Message "Non-Tenant users exist on Unity Connection"

When a tenant creation API fails on a freshly installed system, do the following:

Try to create tenant in Unity Connection that is having users of any other partition, the following error displays:
"Invalid parameter. Parameter = [Non-Tenant users exists on Unity Connection. Cannot proceed with Tenant creation.], Value = [tbl_user]"

**Troubleshooting Problems While Integrating with Call Manager**

See the following sections:

**Hearing the Fast Busy Tone on Dialing the Pilot Number**

You may hear the fast busy tone while dialing the pilot number in the following two cases:

- Ports are busy or locked
- Ports required reset

Do the following:

1. Check on Cisco Unity Connection Administration if any ports require a reset.
2. In case you find any port group that requires a reset then login to Cisco Unity Connection Administration and go to the Port Groups page.
3. If for any port group, value for the Needs Reset field is Yes, then reset the port group.
4. To investigate if ports are busy:
   - Check if ports are busy or number of incoming calls is significantly high in peak hours only or all the time. Based on the tenant's requirement there might be a need to add additional ports.
   - Check Unity Connection phone system: Check ports in Use Counter using the Real-Time Monitoring Tool (RTMT) to see if ports are busy.
   - The ports may be marked busy even if the ports are locked.
   - To verify, check using the RTMT if the port frees up after a call ends and it answers other incoming calls.
   - Check the CUC Phone System: Check the Ports Locked counter for any locked ports. You can reset the port to resolve the port lock issue.

The Ports locked counter in RTMT can be checked in the CUC Phone System counter.

**Hearing the Error Message - "The system is temporarily unable to complete your call" on Dialing the Pilot Number**

To Resolve Issues When there are No Appropriate Routing Rules in Unity Connection

**Step 1**
Enable Threads(11) and Ports(13) level Micro Traces for Arbiter on Cisco Unity Connection Serviceability. Check the diag_CuCsMgr_* .uc log file for the phone system:

'Failed to find routing rule=<PhoneSystem_1>'

where "PhoneSystem_1" is the name of the phone system

**Step 2**
For details on how to view diagnostic traces, see the Using Diagnostic Traces for Troubleshooting, on page 1 section.

**Step 3**
In case, no routing rules exist for the tenant, you can add them using the POST operation on the routing rules API. To identify that which type of routing rules (direct or forward) need to be added, you can use the Port Status Monitor.
If the Port Status Monitor displays that the call does not contain a redirecting ID and value for the Reason field is direct, then Direct Routing Rule is added else add the Forward Routing Rule.

Step 4

If routing rule condition has been removed or is missing from a routing rule on Unity Connection then the routing rule that comes later in the list, is never reached. To check or to investigate the issue:

1. Check if tenant's phone system is added as a routing rule condition in the routing rules for that tenant. For more information refer to the Routing Rule Condition APIs available at http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_APIs.
2. Enable the Micro Traces for Routing Rules and "Thread (11) and Ports(13)" for Arbiter on Cisco Unity Connection Serviceability and check the logs for any errors or issues.
3. Check the phone system configuration like phone system, port groups, ports and SIP security profile for Unity Connection. You can check the following:
   • Verify that the port number specified in SIP Trunk profile on Cisco Unified Communications Manager and the Port Group on Unity Connection are same.
   • Verify that SIP Trunk Security Profile on Cisco Unified Communications Manager has the correct incoming port number.
   • Verify the Cisco Unified Communications Manager IP address or hostname specified in port group on Unity Connection.

---

**Troubleshooting Problems with Migration**

See the following sections:

"Mailbox could not be loaded" Error Shows Up

If the error "Mailbox could not be loaded" shows up for one or more subscribers on Web Inbox after migrating data from a multi-tenant Unity Connection to another multi-tenant Unity Connection, do the following:

Check if the setting required for mailbox access may be lost during migration. To enable it back, do the following:

1. You need the object ID of the class of service for each subscriber and run the following GET request to get the class of service object ID:

   https://<connection-server>/vmrest/users?query=(Alias%20is%20<UserAlias>

2. Send a PUT request to the URI below to enable the setting:

   https://<connection-server>/vmrest/coses/<CosObjectId>

---

SMTP Proxy Address Not Updated on Unity Connection for One or More Subscribers After Migration

1. Look for the errors or warnings in the log files after migration at the following location:
   <COBRASInstallationDirectory>/logs
2. Check whether any subscriber has the same SMTP proxy address by sending a GET request to the URI:
https://<connection-server>/vmrest/smtpproxyaddresses?query=(SmtpAddress%20is%20<SmtpProxyAddress>)
Here, <SmtpProxyAddress> is the field for which the update failed.

3. Run the HTTP GET request below to get the SMTP Proxy addresses URI for the subscriber(s):
   https://<connection-server>/vmrest/users?query=(ObjectId%20is%20<UserObjectId>)

4. Perform an HTTP POST operation on the URI to create the SMTP proxy address and associate it with
   the object ID of the user:
   https://<connection-server>/vmrest/smtpproxyaddresses

### Hearing a Wrong Post Greeting Recording for Users Belonging to a Tenant

If you are hearing a wrong post greeting recording for users belonging to a tenant, do the following:

1. Check if the post greeting recording with the same name already exists in the Unity Connection.
2. Look for the errors or warnings in the log files after migration at the following location:
   <COBRASInstallationDirectory>/logs
3. Administrator can pick the missing recording from the backup of the destination Unity Connection, or
   else re-recording needs to be done.

### Getting Incorrect Time for Incoming or Outgoing Messages

In COBRAS migration, for any subscriber if timezone in the source Unity Connection is set to system default
timezone then after migration in the destination Unity Connection, it would be set to the timezone that the
tenant was created with.

To set it right, do the following:

1. Get the list of users belonging to the tenant using the URI:
   https://<connection-server>/vmrest/users?query=(Alias%20is%20<UserAlias>)

2. Send an HTTP PUT request to the following URI in order to set the time zone for the user to system
default time zone:
   https://<connection-server>/vmrest/users/<UserObjectId>

### Get Incorrect Language for the Incoming or Outgoing Users

In COBRAS migration, for any subscriber if language in the source Unity Connection is set to system default
language then after migration, in the destination Unity Connection, it would be set to the language that the
tenant was created with.

To set it right, do the following:

1. Get the list of users belonging to the tenant using the URI:
   https://<connection-server>/vmrest/users?query=(Alias%20is%20<UserAlias>)

2. Send an HTTP PUT request to the following URI in order to set the timezone for the user to system default
timezone:
   https://<connection-server>/vmrest/users/<UserObjectId>
Troubleshooting Phone View

- Problems with Phone View, on page 231
- Using Traces to Troubleshoot Phone View Issues, on page 233

Problems with Phone View

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 Configured Incorrectly, on page 231 section.
- The user phone configuration is not correct. See the User Phone Configuration Not Correct, on page 232
- The phone system integration is configured incorrectly. See the Phone System Integration Configured Incorrectly, on page 232

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 Phone View" section of the System Requirements for Cisco Unity Connection Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucs.sysreqs.html.

Application User Configured Incorrectly

The problem may be caused by the incorrect configuration of the application user on the Cisco Unified Communications Manager server.

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 Phone Configuration 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.

Phone System Integration Configured Incorrectly

The problem may be caused by the incorrect configuration of the Cisco Unified CM phone system integration in Cisco Unity Connection Administration.

To Verify the Configuration of the Cisco Unified Communications Manager Phone System Integration

Step 1 In Cisco Unity Connection Administration, expand Telephony Integration, then select Phone Systems.
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 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 and select Save.
To Verify the Configuration of the User

**Step 1** In Cisco Unity Connection Administration, expand Users, then select Users. On the Search Users page, select the name of the user.

**Step 2** On the Edit User Basics page, on the Edit menu, select Phone Menu.

**Step 3** On the Phone Menu page, under Finding Messages with Message Locator, confirm that the Enable check box is checked.

**Step 4** Confirm that the Enable Phone View check box is checked and select Save.

Using Traces to Troubleshoot Phone View Issues

You can use traces to troubleshoot phone view issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Using Diagnostic Traces for Troubleshooting, on page 1 section.
Troubleshooting MediaMaster

- Media Master Does Not Display or Function Correctly in Unity Connection Applications, on page 235
- Using the Phone Device for Playback and Recording in Media Master, on page 236
- Problems Opening a File in the Media Master When Saved on a Workstation, on page 238

**Media Master Does Not Display or Function Correctly in Unity Connection Applications**

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. The Media Master 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 Unity Connection.)

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 the Web Browser to Access the Cisco PCA" section in the "Setting Up Access to the Cisco Personal Communications Assistant" chapter of the User Workstation Setup Guide for Cisco Unity Connection, Release 11.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 [https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwxs.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwxs.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 Unity 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 Unity 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/installed.jsp. 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/en/. 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/en/.

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 Device for Playback and Recording in Media Master

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 Unity Connection extension of the user).

The phone device sends requests over the network to the 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 Unity 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.

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.

  ![Note](image)

  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 Updating the Media Master Software, on page 238.

- **No phone system is designated to handle TRAP connections** - By default, the first phone system that is integrated with Unity 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

Follow the steps in the Designating a Phone System to Handle TRAP Connections, on page 238 section.
Updating the Media Master Software

Step 1  Close all browser windows.
Step 2  Depending on your operating system, do one of the following:
   • For Windows 7 and later, start the Java control panel by selecting Control Panel > Java.
   • For Red Hat Linux and Mac OS X, start the Java control panel found in $JAVA_HOME/bin\ControlPanel.
Step 3  On the General page, under Temporary Internet Files, select Settings.
Step 4  In the Temporary Files Settings dialog box, select Delete Files.

This clears the cached files. The Media Master resource files are downloaded the next time you visit a Cisco PCA or Cisco Unity Connection Administration page that contains the Media Master.

Designating 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 Saved on a Workstation

When you attempt to use a previously recorded WAV file (for example, an announcement that was recorded earlier) rather than making a new recording 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.

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 using a phone or a computer microphone.

Note  When Unity Connection is configured to record in the G.729a audio format, the Media Master functions correctly for recording and playing recordings using a phone or a computer microphone.
Troubleshooting Media Player (Release 11.5 (1) and later)

This chapter contains the troubleshooting scenarios of new Media Player with resolution.

- Troubleshooting Media Player (Release 11.5 (1) and later), on page 239

Troubleshooting Media Player (Release 11.5 (1) and later)

This chapter contains the troubleshooting scenarios of new Media Player with resolution.

Using the Phone Device for Playback and Recording in Media Player

The Media Player supports the phone as a playback and recording device. The phone device is always available to users. Using Number or URI field, users can configure the active phone number for the phone device (the default value is the primary Unity Connection extension of the user).

The phone device sends requests over the network to the 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.

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 Player is not the expected number** - Confirm that the active phone number specified in the Media Player is correct. To do this, check the Active Phone Number value for the Primary Extension or Other Number in the Number or URI field on the Media Player.

- **No phone system is designated to handle TRAP connections** - By default, the first phone system that is integrated with Unity Connection is designated to handle TRAP connections for the Media Player. 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

  Follow the steps in the Designating a Phone System to Handle TRAP Connections section.

### Designating a Phone System to Handle TRAP Connections

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unity Connection Administration, expand Telephony Integrations, then select Phone System.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Search Phone Systems page, select the name of the phone system that you want to handle TRAP connections.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Phone System Basics page, check the Default TRAP Switch check box and select Save.</td>
</tr>
</tbody>
</table>

### Problem Uploading a File in the Media Player

When you attempt to use a previously recorded WAV file (for example, an announcement that was recorded earlier) rather than making a new recording using a phone or computer, the Media Player may display the following error message while saving the page:

"Audio format not supported"

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.
- Make the recording using a phone.

You must Save the page after uploading the WAV file on the Media Player.
Unknown Error Appears while Using Media Player

While using Media Player for record, play, upload and download, the Media Player may display the following error message:

"Unknown error. Please contact to System Administrator"

If you receive the above error message, you need to enable the VMREST (all levels) traces and see the `diag_Tomcat_*.uc` log file to troubleshoot the problem.
Unknown Error Appears while Using Media Player
Troubleshooting SNMP

Cisco Unity Connection supports Simple Network Management Protocol (SNMP) to provide standard network management. Unity Connection SNMP uses the SNMP Master Agent service in Cisco Unified Serviceability and the Unity Connection SNMP Agent service in Cisco Unity Connection Serviceability.

Note

Unity Connection SNMP supports CISCO-UNITY-MIB from Cisco Unity.

• Problems with SNMP, on page 243
• Using Traces to Troubleshoot SNMP Issues, on page 244

Problems with SNMP

Use the troubleshooting information in this section if you experience problems with SNMP.

SNMP Master Agent Service 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 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 Unity 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 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 is restarted, select OK.

### Using Traces to Troubleshoot SNMP Issues

You can use traces to troubleshoot SNMP issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Using Diagnostic Traces for Troubleshooting, on page 1.
Troubleshooting Multi-Server Certificate

Cisco Unity Connection supports Multi-server Subject Alternate Name (SAN). See the following sections for information on troubleshooting problems with Multi-server certificates.

- Initial Debugging and Identifying Topology Details, on page 245

Initial Debugging and Identifying Topology Details

Initial Debugging

- Identify the hostname of both the publisher and subscriber nodes in the Unity Connection cluster.
- Identify the node from which the CSR was generated and pushed.
- Identify the node from which the certificate was uploaded.
- Ensure that the Cisco Tomcat and Platform Administrative Web Service (PAWS) are running.

Note

You can use the utils service list CLI command to list the running services.

Collecting Log Files


CLI commands to List and Get Log Files

- CLI command to list the log file is file list<file name>
- CLI command to get the log file is file get<file name>

Required Log Files

There are two log files that need to be collected for analyzing issues with Multi-server Certificate.
• Cisco Tomcat.
• Connection Branch Sync Service.

**CLI Commands examples**

Below are the CLI command examples to list and collect the log files.

• CLI command to list the log files:
  • file list activelog cuc/diag_Tomcat*
  • file list activelog cuc/diag_CUCE.Sync*

• CLI command to collect the log file:
  • file get activelog cuc/diag_Tomcat_00000001.uc
  • file get activelog cuc/diag_CUCE.Sync00000001.uc

After analyzing the log files, if you cannot resolve the problem, contact Cisco TAC.