Cisco Unified Workforce Optimization

Quality Management Troubleshooting User Guide
Version 10.0(1)
First Published: November 30, 2013
Last Modified: October 27, 2014

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

Book Title

Contents

Recording Monitoring Error Messages 55

Troubleshooting Issues 71

Introduction

This document explains how to troubleshoot Cisco Unified Workforce Optimization Quality Management.

The troubleshooting information in this document includes:

- How to locate each service's configuration, log, and debug files.
- How to implement logging, which you can use to monitor your Quality Management environment and troubleshoot issues.
- How to recognize and resolve some of the most common error conditions.

Refer to this document when you need to troubleshoot issues.

References

The following guides are available:

- *Cisco Unified Workforce Optimization Quality Management Application User Guide*
- *Cisco Unified Workforce Optimization Quality Management Administrator Guide*
- *Cisco Unified Workforce Optimization Quality Management CAD Integration Guide*
- *Cisco Unified Workforce Optimization Quality Management Error Code Dictionary*
- *Cisco Unified Workforce Optimization Quality Management Installation Guide*
- *Cisco Unified Workforce Optimization Quality Management Troubleshooting Guide*
- *Cisco Unified Workforce Optimization Quality Management Release Notes*

Service Names and Executables

The following table lists the services installed with Quality Management.

Table 1. Services and executables on the Quality Management server

Service Name	Executable
Quality Management CTI Service	ctiservice.exe
Quality Management Data API Service	datapa.exe
Quality Management DB Cleaner Service	dbcleaner.exe
Quality Management DB Proxy Service	dbproxy.exe
Quality Management Jetty Service	jetty.exe
Quality Management Mana Service	mana.exe
Quality Management Monitor Service	MonitorServer.exe
Quality Management Network Recording Service	RecordServer.exe
Quality Management Sync Service	sync.exe
Quality Management Upload Controller	UploadController.exe
PROXY Pro Gateway Service	PgSvc.exe
Quality Management MediaSense Subscription Service	mssubservice.exe

The following table lists the services for Quality Management that appear in the Windows Services utility on the client desktop.

Table 2. Services and executables on the Quality Management client machine

Service Name	Executable
Quality Management Desktop Recording Service	DesktopRecordServer.exe
Windows Media Player Network Sharing Service	WMPNetwk.exe

Registry Entries

Quality Management modifies Windows registry when you install Quality Management on a machine.

Site Setup Registry Entries

The location of the site setup registry is:

HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\QM\Site Setup

The following table shows site setup registry entries for Quality Management.

Table 3. Site setup registry entries

Value	Type	Description
APP VERSION	string	Version of the Quality Management software
Base Host 1	string	IP address of the Quality Management server
BRAND	string	Brand of Quality Management software installed 0: Cisco 1: Calabrio
CALLCENTERLANG	dword	Software localization language
Connection Timeout	dword	Maximum time in seconds before a connection attempt times out
Context URL	string	
FirstRun	dword	1: System Configuration Setup has run to completion 0: System Configuration Setup has not run to completion
INSTALL DIRECTORY	string	Root directory of the Quality Management installation
INSTALLDIR	string	Base installation directory for the Quality Management software

Table 3. Site setup registry entries (Continued)

Value	Type	Description
IOR HOSTNAME	string	Host name or IP address of the Quality Management services
MONITOR DEVICE	string	The ID of the network adapter used to filter Real-time Transport Protocol (RTP) packets for voice recording
ProductCode_Server	string	A Unique Identification (UID) for this installation that is required for Desktop Recording
Root URL	string	Root URL of the Quality Management installation that is used to communicate with the database and should always be /api/rest
Service Password	string	An encrypted password that is used for API communication
Service User	string	The user that is used for API communication
Surrogate Host 1	string	Host name or IP address of the Quality Management Data API service
Surrogate Host 2-5	string	Host name or IP address of the backup Quality Management Data API service
Surrogate Port 1	dword	Quality Management Data service port number
Surrogate Port 2-5	dword	Backup Quality Management Data services port numbers

Logs and Debugging

The default settings are usually sufficient for debugging issues in your Quality Management environment. However, TAC occasionally encounters issues that require more scrutiny. Understanding how Quality Management implements logging will help you work with TAC to resolve your issues more quickly and easily.

With Quality Management you can pick and choose which log statements are written and where these statements are written. To identify which log statements Quality Management should write, you define the logging level, or threshold, that selects only the log statements you want to see. You can also identify the destination where the log statements are written.

Every log statement is associated with a specific threshold, which has to do with the severity of the event the statement describes and the amount of information the statement contains.

These thresholds are organized in order of their severity. For example, the WARN threshold is higher than the INFO threshold, which in turn is higher than the DEBUG threshold.

Applications and services use logging to report their current status, including problems. Each application and service creates two files:

- **Log files** (LOG file extension): The log files contain status messages and, if problems occur, warning and other error messages. A log file associates each message with an error code. See the *Error Code Dictionary* for more information on error codes.
- **Debugging files** (DBG file extension): The debugging files are empty when you disable debugging. When you enable debugging (the default setting), the files contain diagnostic information that can help resolve issues.

The following table shows the location of the log and debugging files.

Table 4. Log and debugging files location

Where Used	Folder Location
Server Computer	C:\Program Files\Cisco\WFO_QM\log
Desktop	C:\Program Files (x86)\Cisco\WFO_QM\log (for Windows 7) C:\Program Files (x86)\Cisco\WFO_QM\log (for Windows XP)

The default configuration settings limit each log and debugging file to a maximum of 10 MB and 20 rolling files for Quality Management services and 5 MB and 5 rolling files for applications. For example, when a service's log or debug file reaches 10 MB, Quality Management closes and renames it, and then starts a new debug file.

C++ configuration files (CFG extension) produce logs using this numbering scheme:

```
<name>0001.log
<name>0002.log
```

Quality Management initially creates the <name>0001.log. When the <name>0001.log is full, Quality Management creates the <name>0002.log. When the <name>0002.log is full, Quality Management clears the <name>0001.log and reuses it. The process repeats as Quality Management fills each log. Only one of the two logs is active at any given time.

Java configuration files (properties extension) produce logs using this numbering scheme:

```
<name>.log
<name>.log.1
```

Quality Management creates the <name>.log file. When it is full, Quality Management saves it the <name>.log.1 file. The <name>.log file is always the active file.

Debug logs follows the same numbering scheme, but it uses the *.dbg file extension.

Log Message Formats

The various log and debug file messages use the following message formats. An example follows each message format.

C++ and Java *.log file messages

```
<timestamp> <level> <error code> <error text>
```

```
2007-02-28 09:29:11.723 INFO ABCD1234 Successfully
launched update.
```

C++ *.dbg file messages

```
<timestamp> <level> [<thread ID>] <text>
```

```
2007-02-28 14:51:13.723 DEBUG [0xaa8]
CSqmcApiBase::_doRecovery: Connected to QM Controller.
```

Java *.dbg file messages

```
<timestamp> <level> [<thread
name>|<class>#<method>:<line> ] <text>
```

```
2007-04-07 15:04:31.954 STACK [Thread-2|Init#run:113]
Started.
```

Java (log4j) *.log file messages

```
<timestamp> <level> [<thread name> [<class>] <text>
```

```
2007-04-07 14:54:00,0670 INFO[Thread-2]
[com.calabrio.morepackages.Init] Started.
```

Configuration Files

Each application and service has an associated configuration file that controls logging and debugging. You can edit these files in a text editor such as Windows Notepad to change the logging and debugging parameters.

CAUTION: Edit configuration files only as described in this section. Improper changes can result in logging and/or program failure, including the possible loss of data. It is recommended that you make a safety backup of any file you edit before you make changes to it.

The C:\Program Files\Cisco\WFO_QM\config folder on the client or Base server contains most of the configuration files except where noted in the following tables.

Table 5. Quality Management configuration files and log files on the server

Service / Application	Configuration File	Log File
Base Services		
Data API service	datapa.properties	datapa.log datapa.dbg.N

Table 5. Quality Management configuration files and log files on the server

Service / Application	Configuration File	Log File
Jetty service	jetty.properties	jetty-request-YYY_MM_ DD.log jetty.dbg
	C1Surrogate.properties	C1SurrogateNNNN.log C1SurrogateNNNN.dbg
	exportedRecordingServlet.properties.	exportedRecordings.log exportedRecordings.dbg
File Transfer Servlet (FTS)	fts.properties	fts.log fts.dbg
MANA service	manaEmergency.properties	mana.log mana.dbg.N
	manaservice.properties	
Sync service	DirAccessSynSver.cfg	DirAccessSynSvrNNNN.log, DirAccessSynSvrNNNN.dbg
	sync.properties	sync.log sync.dbg
DB Sync service	dbsync.properties	dbsync.log dbsync.dbg
ContactDelete utility	contactdelete.properties	ContactDelete.log ContactDelete.dbg
Configuration Setup	postinstall.properties	postinstall.log postinstall.dbg
	sitedefaults.properties	
	platform.properties	
Backup and Restore	bars.properties	bars.log bars.dbg
Quality Management Administrator	admin.properties	admin.log admin.dbg
Database Services		

Table 5. Quality Management configuration files and log files on the server

Service / Application	Configuration File	Log File
DB Cleaner service	dbcleaner.properties	dbcleaner.log dbcleaner.dbg
DB Proxy service	dbproxy.properties	dbproxy.log dbproxy.dbg
Site Upload Server		
Jetty service	jetty.properties	jetty-request-YYY_MM_ DD.log jetty.dbg
	C1Surrogate.properties	C1SurrogateNNNN.log C1SurrogateNNNN.dbg
	exportedRecordingServlet.properties.	exportedRecordings.log exportedRecordings.dbg
File Transfer Servlet (FTS)	fts.properties	fts.log fts.dbg
Upload Controller service	dbupload.properties	dbUpload.log dbUpload.dbg
	UploadController.cfg	UploadControllerNNNN.log, UploadControllerNNNN.dbg
Load-balancing Subscription Service (Signaling Services)		
CTI service	ctiservice.properties	ctiservice.log.N ctiservice.dbg.N
	CTIservice.cfg	CTIserviceNNNN.log CTIserviceNNNN.dbg
MediaSense Subscription service	mssubservice.properties	mssubservice.log mssubservice.dbg
Reconciliation Services		
Contact Reconciliation service	reconciliation.properties	reconciliation.log reconciliation.dbg

Table 5. Quality Management configuration files and log files on the server

Service / Application	Configuration File	Log File
ICM Reconciliation service	icmrecon.properties	icmrecon.log icmrecon.dbg
Recording Services		
Network Recording service	RecordServer.cfg	RecordServerNNNN.log RecordServerNNNN.dbg
Voice Record server	VoiceRecordServer.cfg	
Monitoring Services		
Monitor service	MonitorServer.cfg	MonitorServerNNNN.log MonitorServerNNN.dbg
Additional Services / Applications		
License Servlet	licensing.properties	licensing.log licensing.dbg
Locale	locale.properties	
Quality Reports	qmr.properties	SQMR.log SQMR.dbg
Recording Controls	recordingcontrols.properties	recordingcontrolsNNNN.log recordingcontrolsNNNN.dbg
Quality Reports	reportConfig.properties	SQMR.log
RECON	recon.cfg	RECONNNNN.log RECONNNNN.dbg
True Update	SplkUpdate.cfg	Calabrio Quality Management Software Update Log.txt (located at C:\Documents and Settings\Local Settings\Temp\)

The following table displays the Quality Management configuration files and log files on the client.

Table 6. Quality Management configuration files and log files on the client

Service / Application	Configuration File	Log File
Quality Management Administrator	admin.properties	admin.log admin.dbg
Configuration Setup	postinstall.properties	postinstall.log, postinstall.dbg
Desktop Recording	DesktopRecordServer.cfg	DesktopRecordServerNNNN.log DesktopRecordServerNNNN.dbg
True Update	splkUpdate.cfg	splkUpdateNNNN.log splkUpdateNNNN.dbg
Media Player	media-player.properties	media-player.log media-player.dbg NOTE: These logs are located in one of the following locations: • XP: C:\Documents and Settings\<username>\log\media-player • Vista: C:\Users\<username>\log\media-player

About Debugging

Quality Management allows you to configure the debugging thresholds that help you diagnose problems. Quality Management enables debugging by default. When enabled, note that the more detail the debugging threshold provides, the slower the performance of your server and the bigger the size of the debug file.

The following table shows the location of the configuration files.

Table 7. Configuration files location

Where Used	Folder Location
Server Computer	..\Cisco\WFO_QM\config

Table 7. Configuration files location (Continued)

Where Used	Folder Location
Desktop	..\Program Files\Common Files\QM\config

Quality Management uses the following configuration files:

- C++ files that use the *.cfg extension
- Java files that use the *.properties extension
- Java files whose file names begins with “log4j”

Each type of file uses a different syntax to enable and disable debugging.

> **NOTE:** Disable debugging when it is no longer needed for diagnostic purposes. Debugging can affect the performance of other applications running on your PC when enabled.

The following table describes the available debugging thresholds.

Table 8. Debugging Thresholds

Threshold	Debugging
DEBUG	Usually sufficient for diagnosing a problem. Does not affect system performance.
CALL	Tracks function entry and exit.
TRACE	Provides a large amount of diagnostic information. May affect system performance.
STACK	Provides only stack traces, which give more debugging information when errors and warnings occur.
DUMP	Provides a very large amount of detailed diagnostic information. Likely to affect system performance.
OFF	Turns off debugging.

Enabling Debugging in Files with a *.cfg Extension

TASK

1. In a text editor, open the desired configuration file.

2. Under the section headed [Debug Log], set the debugging threshold to DEBUG, CALL, TRACE, or DUMP. For example:

   ```
   Threshold=DEBUG
   ```

   ADDITIONAL INFORMATION: The threshold value must be all caps (for example, DEBUG) and there should be no spaces on either side of the equal sign (=).

   The line might already exist or you might have to add a new line.

3. Save the configuration file.

   STEP RESULT: The change takes effect immediately. You do not have to restart the application or service.

Disabling Debugging in Files with a *.cfg Extension

TASK

1. In a text editor, open the desired configuration file.
2. Under the section headed [Debug Log], set the debugging threshold to OFF. For example:

   ```
   Threshold=OFF
   ```

   ADDITIONAL INFORMATION: The threshold value must be all caps (for example, OFF) and there should be no spaces on either side of the equal sign (=).

3. Save the configuration file.

   STEP RESULT: The change takes effect immediately. You do not have to restart the application or service.

Enabling Debugging in Files with a *.properties Extension

TASK

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

   ```
   log4j.rootLogger=<threshold>#com.calabrio …
   ```

3. Replace <threshold> with DEBUG, TRACE, STACK, or DUMP.

4. Locate the line that starts with:

```
log4j.appender.DBG.Threshold=<threshold>#com.calabrio …
```

5. Replace <threshold> with the same value you used in Step 2.

6. Save the configuration file.

STEP RESULT: The change takes effect according to the splk4j.watch.check setting (by default, within 90 seconds). You do not have to restart the application or service.

Disabling Debugging in Files with a *.properties Extension

TASK

1. In a text editor, open the desired configuration file.

2. Locate the line that starts with:

```
log4j.rootLogger=<threshold> …
```

3. Replace <threshold> with STACK.

4. Locate the line that starts with:

```
log4j.appender.DBG.Threshold=<threshold> …
```

5. Replace <threshold> with OFF.

6. Save the configuration file.

STEP RESULT: The change takes effect according to the splk4j.watch.check setting (by default, within 90 seconds). You do not have to restart the application or service.

Enabling Debugging in log4j Files

TASK

1. In a text editor, open the desired configuration file.

2. Locate the line that starts with:

```
log4j.rootLogger=<threshold>
```

3. Replace <threshold> with DEBUG or TRACE.
4. Save the configuration file.

STEP RESULT: Restart the application or service for the new setting to go into effect.

Disabling Debugging in log4j Files

TASK

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

```
log4j.rootLogger=<threshold>
```

3. Replace <threshold> with INFO.
4. Locate the line that starts with:

```
log4j.appender.DBG.Threshold=<threshold>
```

5. Replace <threshold> with DEBUG.
6. Save the configuration file.

STEP RESULT: Restart the application or service for the new setting to go into effect.

Collecting Log and Debugging Files

Cisco provides the following tools to collect logs and debugging files:

- Log Tool—use this tool to collect logs and debugging files from the agent and server machines. See Log Tool for more information.
- Recording Client Console (RECON)—use this tool to set the logging levels on agent desktops, gather logs from agent desktops, and track the version of the recording client installed on the agent desktop. See RECON for more information.

Log Tool

Log and debugging files can be collected from agent and server machines and copied to one location using the Log Tool. The Log Tool is a self-contained executable that can

be added to any server within your network. It makes compiling logs for troubleshooting and for sending to TAC easier and faster.

The Log Tool is added to a single server within your network and can operate using one of two methods, depending on your contact center environment.

- Running the Log Tool from a Central Server (Method 1): This method might be used in environments with less stringent security. The Log Tool is set up on a central network server. The command to execute the Log Tool occurs on this server and log collection is run concurrently on designated agent and server machines. The log and debugging files are collected and copied to a designated location.
- Running the Log Tool from Agent Machines (Method 2): This method might be used in environments with tighter security. Some security environments prevent Method 1 from working due to operating system features being disabled or ports being closed. The Log Tool is set up on a central network server and a shortcut to the Log Tool is placed on each agent or server machine from which you want to collect logs. The command to execute the Log Tool comes from each agent machine, and the Log Tool is launched from the central server. The log and debugging files are collected and copied to a designated location.

The Log Tool can be setup as a scheduled task in conjunction with either method.

Adding the Log Tool to Your Network

No installer is required to execute the Log Tool. You simply copy and paste the appropriate files to a designated server in your network. The files to copy depend on what method of operation you want to use.

Log Tool Setup for Method 1

TASK

1. Copy the following files to the designated network server:
   - CalabrioLogTool.exe
   - Configuration.txt
   - PsExec.exe
2. Copy TurnOffUACDlgForAdmin.reg to all agent and/or server machines that run Windows Vista, Windows 7, and Windows Server 2008 operating systems.

   ADDITIONAL INFORMATION: Windows Vista, Windows 7, and Windows Server 2008 operating systems have a feature called User Account Control. This displays a dialog box prompting the user to allow certain processes to execute. The

TurnOffUACDlgForAdmin.reg file suppresses this prompt to eliminate interference with the Log Tool.

Log Tool Setup for Method 2

TASK

1. Copy the following files to the designated network server:
   - CalabrioLogTool.exe
   - Configuration.txt
2. Create a shortcut to the Log Tool on each agent and/or server machine from which you want to collect logs. See "Running the Log Tool from Agent Machines (Method 2)" on page 38 for more information.

Configuring the Log Tool

The steps to configure the Log Tool are the same for both methods of operation. You can save your settings at any point by clicking the Save Configuration button.

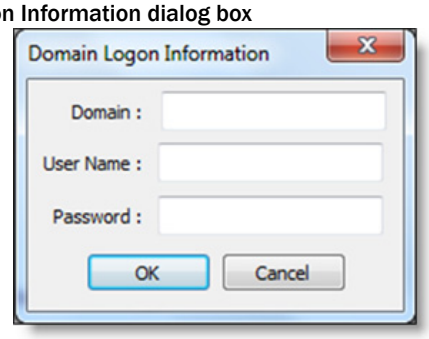
Configuring the Global Tab

TASK

1. To launch the Log Tool on the network server, double-click CalabrioLogTool.exe.

   STEP RESULT: The Domain Logon Information dialogue box (Figure 1) the first time you launch the Log Tool.

Figure 1. Domain Logon Information dialog box



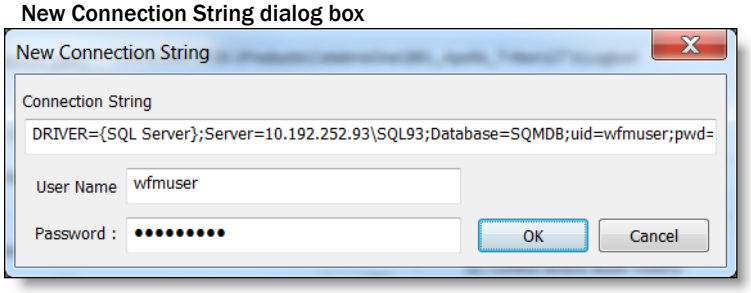
2. Enter the domain and your administrator credentials, and then click OK to dismiss the Domain Logon Information dialog box.

   STEP RESULT: The Calabrio Log Tool window appears.

3. From the Calabrio Log Tool window, click the Global tab (Figure 3 on page 33), and then click Configure.

STEP RESULT: The New Connection String dialog box appears (Figure 2).

Figure 2. New Connection String dialog box



4. Enter the connection string in the following form:

```
DRIVER={SQL Server};Server=<database
IP>\<instance>;Database=<database
name>;uid=<username>;pwd=secret;
```

where:

<database IP> is the IP address of the server that contains the SQL server.

<instance> is the name of the SQL instance.

<database name> is the name of the SQL database.

<username> is the username you use to access this database.

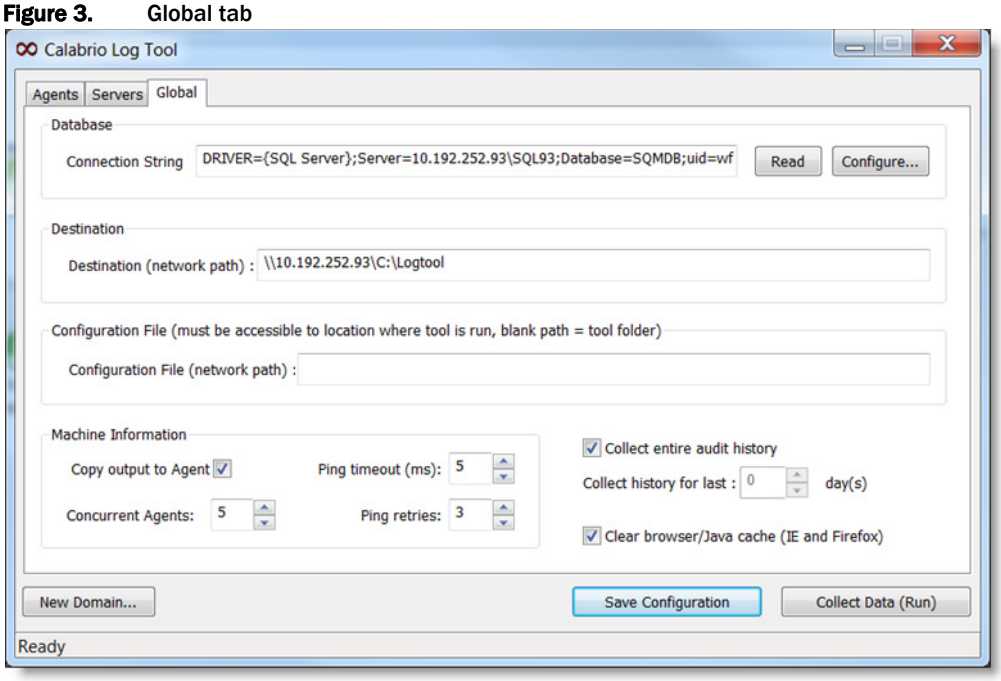
5. Enter your username and password and then click OK to save your changes and dismiss the dialog box.

6. Click Read.

ADDITIONAL INFORMATION: The bottom left corner of the Log Tool window says Ready if you successfully accessed the database or Open Database Failed if you did not successfully access the database.

STEP RESULT: The Log Tool reads information from the database, and automatically populates the remaining Log Tool tabs.

Figure 3. Global tab



7. In the Destination (network path) field, enter the location where you would like to save the collected logs and files in the following format:

\\<server IP>\<share> or <drive:>\<path>

where:

<server IP> is the IP address of the server to which you want to copy the logs.

<share> or <drive:> is the share or drive where you want to save your collected logs. You must include the letter of the drive followed by a colon.

<path> is the path to the file where the collected logs are saved.

8. Under Machine Information, you can choose one or more of the following options:

   - Create a copy of the collected logs on the agent machine by selecting the Copy output to Agent check box.
   - Specify the time between log collection attempts by entering a number in the Ping timeout (ms): field.
   - Specify the number of machines to collect from concurrently by entering a value in the Concurrent Agents field (installation method 1 only).
   - Specify the number of times to retry log collection by entering a value in the Ping attempts field.

– Clear the internet browser and Java cache on the agent machine by selecting the Clear browser/Java cache (IE and Firefox) check box.

Configuring the Agents and Servers Tabs

TASK

1. On the Calabrio Log Tool window, select the Agents tab or the Servers tab.

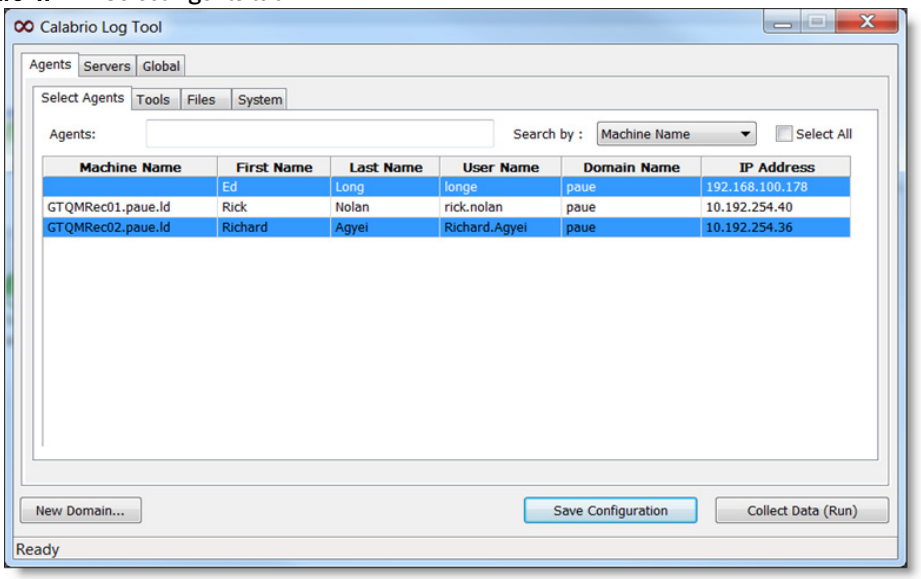
   ADDITIONAL INFORMATION: The configuration steps are the same for both the Agents tab and the Servers tab.

2. Click the Select Agents tab (Figure 4) or the Select Servers tab, and select the machines from which you want to collect logs.

   ADDITIONAL INFORMATION: To select all the machines listed, select the Select All check box.

   To search for a specific machine, choose a search parameter from the Search by drop-down list and type a query in the Agents field.

Figure 4. Select Agents tab

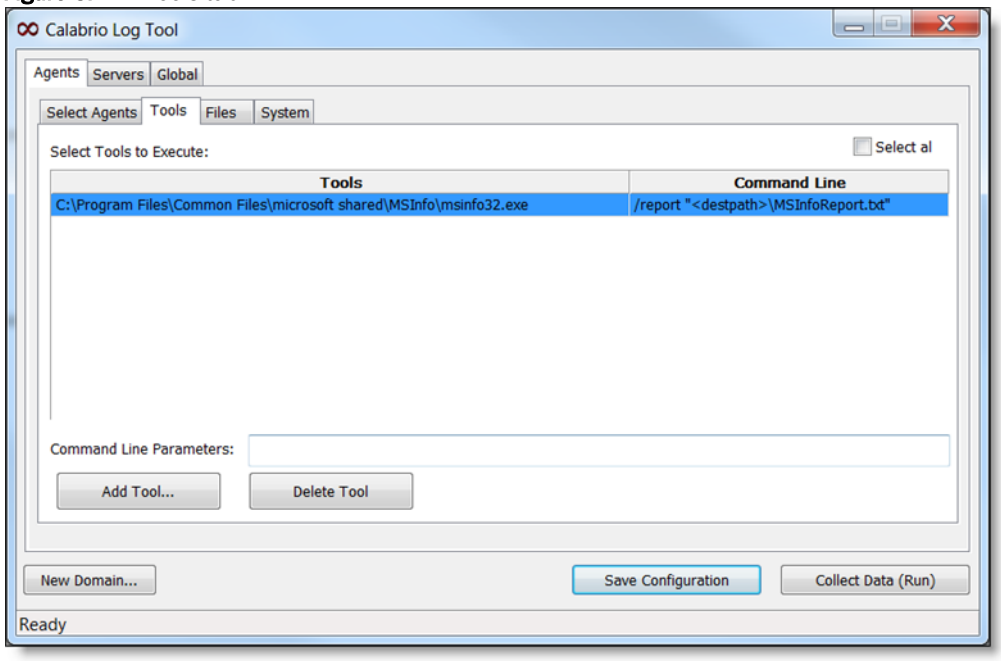


3. Click the Tools tab (Figure 5), and then select the tools to run on each machine.

   ADDITIONAL INFORMATION: By default, msinfo32.exe with the correct command line appears in the Select Tools to Execute table.

The path for the report displayed on this tab is ignored. The report is saved to the destination you specified on the Global tab.

Figure 5. Tools tab

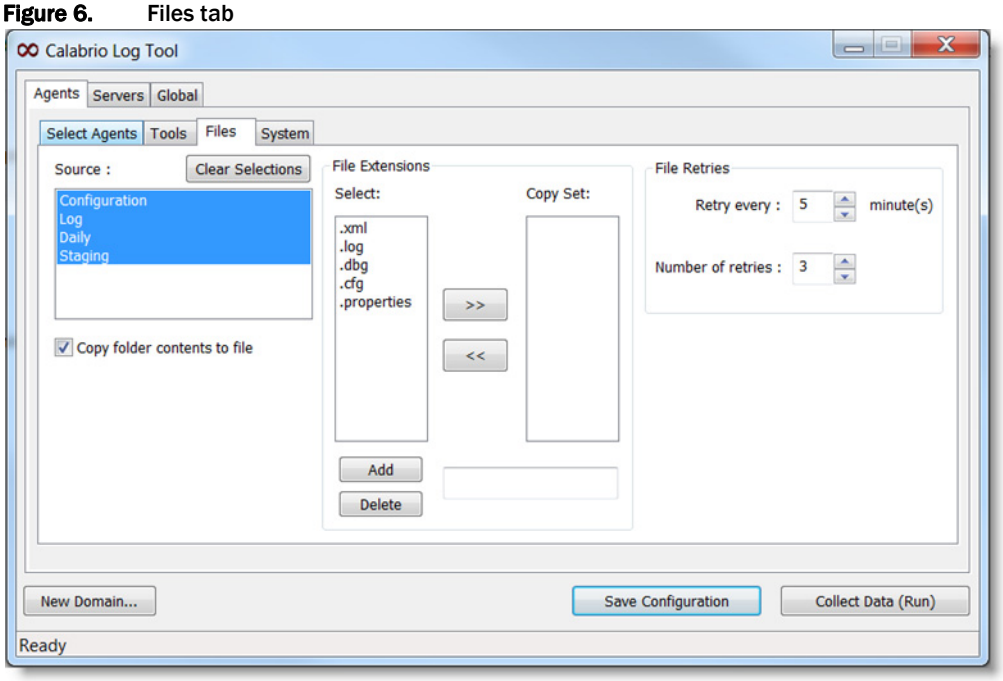


4. Click the Files tab (Figure 6), and then select the types of files you want to collect.

5. In the Source list, select one or more file source locations.

   ADDITIONAL INFORMATION: All files contained in the Configuration or Log source locations are copied to the destination you specified on the Global tab.

Figure 6. Files tab



ADDITIONAL INFORMATION: The Daily and Staging folders no longer appear in 9.1. Files for these source locations will be copied from the Recordings folder.

6. In the File Extensions panel, select one or more file types you want to copy the Select list and click >> to move the file types to the Copy Set list.

   ADDITIONAL INFORMATION: If no file types are listed in the Copy Set list, then all files contained in that source location are copied.

   By default, only .xml files are copied from the Daily and Staging source locations. You can select additional file types by moving them to the Copy Set list.

   To add a file type, enter the file extension in the field at the bottom of the File Extensions panel and then click Add. You can remove a file type by selecting from the Select list and then clicking Delete.

7. To create a list of all files copied from the selected sources in the output log file, select the Copy Folder Contents to File check box.

8. Specify the number of times the Log Tool will try to copy files in the Number of Retries field and the interval between attempts in the Retry Every field.

   ADDITIONAL INFORMATION: The Log Tool might encounter files that cannot be copied because they are in use by the machine from which they are being collected. The number of times the Log Tool attempts to copy these files is determined by the value specified in the Number of Retries field.

9. Click the System tab (Figure 7).

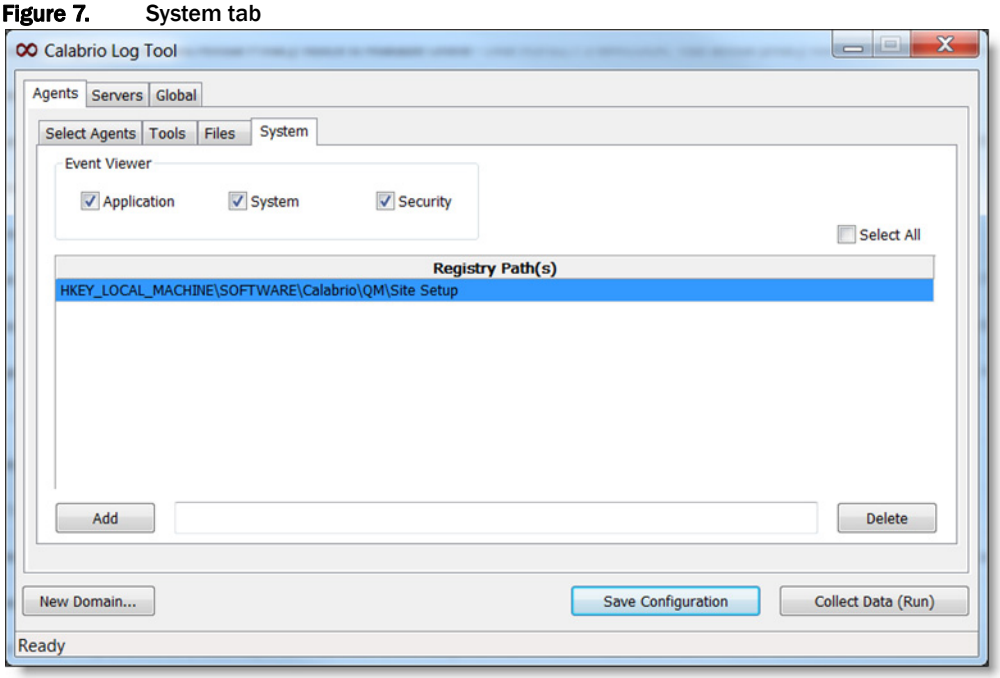
10. Select the one or more of the following event logs in Event Viewer panel:

    - Application
    - System
    - Security

11. Choose one of the following options:

    - To select all the registry entries listed under Registry Path(s), select the Select All check box.
    - To add registry entries, enter the registry path in the field and then click Add.
    - To remove registry entries, select one or more registry paths from the list and then click Delete.

Figure 7. System tab



Running the Log Tool

Running the Log Tool from a Central Server (Method 1)

TASK

- On the Calabrio Log Tool window, once configuration is completed, click the Collect Data (Run) button.

STEP RESULT: The Log Tool is launched and begins collecting log and debugging files undetected on the agent and server machines.

Running the Log Tool from Agent Machines (Method 2)

TASK

1. On the Calabrio Log Tool window, once configuration is complete, save your settings by pressing the Save Configuration button. Close the Log Tool.

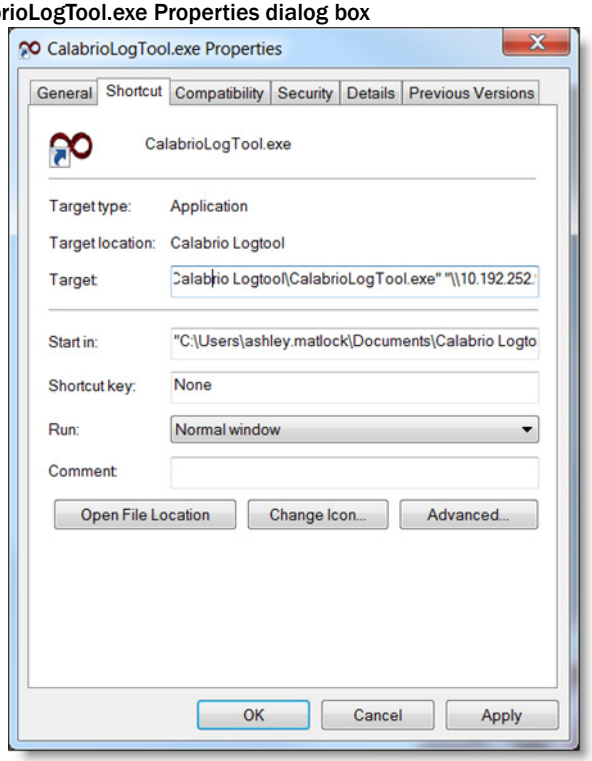
2. On an agent or server machine from which you want to collect logs, create a shortcut to the Log Tool using a network path that points to the Log Tool on the central network server. Use the following format:

   \\<server IP>\<share>\<path>\CalabrioLogTool.exe

3. Right-click the shortcut you just created, and choose Properties from the popup menu.

STEP RESULT: The CalabrioLogTool.exe Properties dialog box (Figure 8) appears.

Figure 8. CalabrioLogTool.exe Properties dialog box



4. On the Shortcut tab, in the Target field, after the final quote symbol, insert a space. Then enter a path to the Configuration.txt file on the network server like the following (including the quotes):

   "\\<server IP>\<share>\<path>\Configuration.txt"

   ADDITIONAL INFORMATION: Use quotes if the path contains spaces.

5. Click OK to save your changes and dismiss the window.

IMPORTANT: You must create a shortcut and configure it on every machine from which you want to collect logs.

6. Run the Log Tool by opening the shortcut on the agent or server machines.

   ADDITIONAL INFORMATION: If the machine you run the Log Tool from was not selected on the Select Agents or Select Servers tabs during the configuration process, then the Log Tool automatically terminates.

Running the Log Tool as a Scheduled Task

The Log Tool can be run as a scheduled task for both methods of operation. This allows for log file collection to occur automatically at predetermined times.

The steps to create a scheduled task vary depending on which version of Windows you use.

Windows XP

For information on creating a scheduled task in Windows XP refer to the following Microsoft Support article (Article ID: 308569) at:

http://support.microsoft.com/kb/308569

Windows Vista

For information on creating a scheduled task in Windows Vista refer to the following Microsoft Windows article at:

http://windows.microsoft.com/en-US/windows-vista/Schedule-a-task

Windows 7

For information on creating a scheduled task in Windows 7 refer to the following Microsoft Windows article at:

http://windows.microsoft.com/en-us/windows7/Schedule-a-task

IMPORTANT: In order for the Log Tool to run as scheduled task, you must set the command line parameter to /x.

RECON

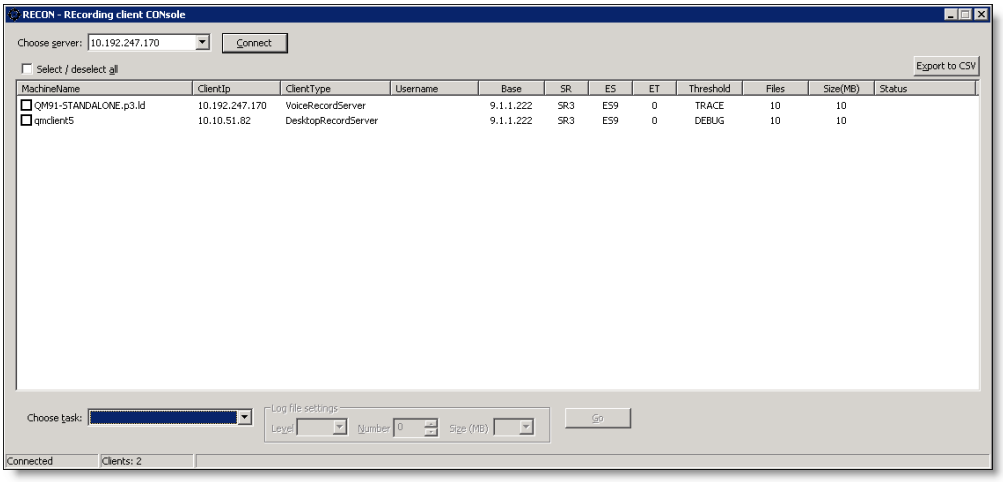
The RECON allows you to set the logging levels on agent desktops and gather logs from agent desktops.

> **NOTE:** You must be a Quality Management administrator to access RECON. If you are using Active Directory, you must belong to the Admin User Group that is configured in the Active Directory Domain Information in Quality Management Administrator.

You can also use RECON to track the version of the recording client installed on the agent desktop.

The RECON.exe is located on the Base server in the following directory:

C:\Program Files\Calabrio\WFO_QM\bin



Field or Button	Description
Choose Server	Choose the IP address or hostname of the Upload Controller.
Connect	Connects to the Upload Controller and populates the RECON table when successful. Once connected, RECON continues to receive DIAGNOSTIC_CLIENT_UPDATE_EVENT messages in real time as recording clients connect to and disconnect from the Upload Controller.
Select/Deselect All	Select this check box to select all agent desktops or clear the check box to deselect all agent desktops in the RECON Table.
Export to CSV	Exports the contents of the RECON table into a CSV file.
MachineName	The machine name of the agent desktop.
ClientIP	The IP address of the agent desktop

Field or Button	Description
ClientType	Identifies the client application type installed on the agent's desktop. The possible values are as follows: • DesktopRecordServer • VoiceRecordServer • ScreenRecordServer
Base	The version of the Quality Management base release on the agent desktop.
SR	The service release number on the agent desktop.
ES	The engineering special number on the agent desktop.
ET	The engineering test number on the agent desktop.
Threshold	The current logging threshold on the agent desktop. The possible values are as follows: • DEBUG • CALL • TRACE • STACK • DUMP • OFF
Files	The number of log files on the agent desktop.
Size (MB)	The size of the log files in megabytes.

Field or Button	Description
Status	The status of the current task. The possible statuses are as follows: • Upload in progress • Upload pending **NOTE:** To cancel a pending upload, right click the row with the Upload pending status and then click Cancel. • Upload succeeded When you run a task, the status for each agent desktop updates one at a time.
Choose Task	Select the machines you want to upload from and then choose from of the following tasks from this drop-down list: • Update log settings fro checked • Upload logs from checked
Level	The debugging threshold level to assign to the agent desktop. The possible values are as follows: • DEBUG • CALL • TRACE • DUMP This field is enabled when you choose Update log settings for checked from the Choose Task drop-down list.
Number	This field is enabled when you choose Update log settings for checked from the Choose Task drop-down list.
Size (MB)	This field is enabled when you choose Update log settings for checked from the Choose Task drop-down list.
Go	Run the selected task against each selected agent desktop. RECON uploads the results of the task one agent desktop at a time.

Configuring the Screen Playback Gateway

After you install the Quality Management and successfully run System Configuration Setup, you must manually configure the Screen Playback Gateway permissions for administrators on the server that hosts the Network Recording service and the server that hosts the Site Upload Server.

This topic applies only to systems that include screen recording (AQM or AQMA license).

Configuring the Screen Playback Gateway Permissions for Administrators

Use this task to configure the Screen Playback Gateway permissions for administrators.

TASK

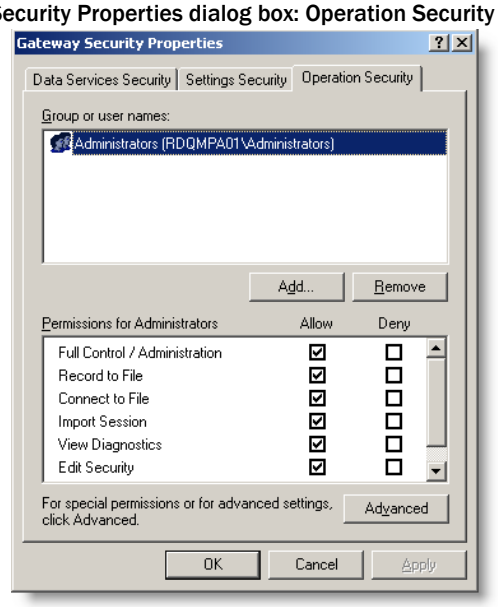
1. On the server that hosts the Network Recording service and the server that hosts the Site Upload Server, launch Screen Playback Gateway Administrator (Start > Programs > Proxy Networks > PROXY Pro Gateway Administrator).

2. In the navigation tree, select the Gateway Security node, and from the right pane, click the Click Here to Change Operation Security link.

3. Click the Operation Security tab.

   STEP RESULT: The Operation Security tab on Gateway Security Properties dialog box appears (Figure 9).

Figure 9. Gateway Security Properties dialog box: Operation Security tab



4. On the Operation Security tab, enable permissions for administrators as follows:

   - On the server that hosts the Quality Management Network Recording service, select the Allow check box for Record to File.
   - On the server that hosts the Quality Management Site Upload Server, select the Allow check box for Connect to File.

5. Click OK.

ContactDelete Utility

The ContactDelete utility (ContactDelete.exe) is a command line tool that resides on the Quality Management server.

The location of the ContactDelete utility is:

...\Cisco\WFO_QM\bin\ContactDelete.exe

Use the ContactDelete utility to permanently delete a specified contact from the database. Note that you must navigate to the bin folder in order to run the ContactDelete utility or it will fail.

When you run this utility on a record, the utility deletes the contact from the calculations and contact lists. Only the log file indicates the deletion of the record. The audit trail does not indicate the deletion of the record. The deletion is permanent—you cannot recover the contact.

A properties file contains the ContactDelete utility's logs. The location of the properties file is:

...\Cisco\WFO_QM\config\ContactDelete.properties

The log and debugging files are:

...\Cisco\WFO_QM\log\ContactDelete.log

...\Cisco\WFO_QM\log\ContactDelete.dbg

Using the ContactDelete Utility

The syntax for this utility is as follows:

ContactDelete.exe <options> <contact ID>

Where:

- <contact ID>—The contact ID of the contact you want to delete.
- <options>—Optional command parameters. The available command parameters are as follows.
  - -h or -help—Displays additional help information and any options.
  - -f or -force—Deletes contact without prompting for deletion confirmation.

Best Practices

Best practices recommendations are listed below.

Deploying Client Applications

The following topics describe best practices for deploying client applications.

Windows Installer Logging

Window Installer logging should be enabled. The installations should be run with the following command:

<client application executable> /l*v <logfile path and name>

where <client application executable> is the name of the client application's executable file and <logfile path and name> is the name and location of the log file.

EXAMPLE: Calabrio Monitoring and Recording Recording.msi /l*v c:\installer.log

> **NOTE:** Specify the location for the logfile path and name where you have write permission.

This ensures that any loggable issues are captured efficiently.

Deployment

Each installation package should be deployed using its own deployment package. Using separate packages offers faster isolation of potential issues than does a composite deployment package.

Installation and Uninstallation Deployment Packages

The deployment engineer should create and test both an installation and uninstallation deployment package.

Live Monitoring Error Messages

This topic explains the messages that might appear in Live Monitoring when attempting to live-monitor calls. These messages are displayed temporarily at the top of the page as status messages. All status messages appear in the Status window (displayed when you click the Status button) for as long as the Live Monitoring application is open.

All Live Monitoring error messages are prefixed with "Live Monitor ('<first name>' '<last name>'", where <first name> and <last name> are the first and last name of the person of whom the monitoring attempt is made.

In all cases when these error messages are displayed, the call cannot be monitored.

Common Live Monitoring Error Messages

There are no active calls on the target device.

Description. This error is unlikely, because Live Monitoring should prevent attempts to monitor users who do not have an active call. However, there could be a race condition where the call ends at the same time a request is made to monitor the call.

Action. Try the following actions.

- Monitor the call again.
- Refresh the browser page.

The provided extension cannot reach the extension of the user to be monitored.

Description. The monitor calling search space for the extension entered in My Extension does not include the agent line or device partition to allow monitoring the agent.

Action. See the documentation for Unified CM for more information on monitor calling search space and device partitions.

Timeout error.

Description. The request to monitor was sent, but no response was received after 30 seconds. This is unlikely, but probably due to a very busy system that is slow in other ways.

Action. Try to monitor the agent again. You might have to wait until the system is not so busy.

Live Monitoring Error Messages for Cisco Unified CCX

The extension is not configured properly for silent network monitoring.

Description. You tried to monitor a user who is not configured for recording. This error is uncommon because Live Monitoring should not present users who are not configured for recording. It could potentially happen if the user configuration is actively being edited while Live Monitoring is running.

Action. Reload Live Monitoring in the browser. If you still receive the error message, check that the user is properly configured for recording and monitoring on both the Unified CM and in Quality Management.

The device to be monitored is not in the provider's domain.

Description. The extension entered in My Extension was not added to the Unified CM application user group that was configured for call monitoring. This application user is referred to as the JTAPI User in System Configuration Setup.

Action. Add the supervisor device to the JTAPI User, and make sure that the JTAPI User has call monitoring privileges.

The provided extension is not a valid extension on the Unified Communications Manager for the user you are trying to monitor.

Description. This is the most common error that can occur. It is due to one of the following:

- You entered a number that does not exist on the Unified CM.

- The Unified CM is configured so that it requires you to enter the entire 10-digit phone number, and you entered only the last four digits (the extension). For example, you entered “5555” but the Unified CM requires “763-555-5555.”
- The number you entered is correct, it exists on your Unified CM, and it is configured correctly. However, the user you are trying to monitor is on a different cluster.

Action. Verify the device number of the user you want to monitor. Make sure that is configured correctly in Unified CM.

The target device is being monitored by someone else, has no built-in bridge, or is unavailable.

Description. This error has two primary causes:

- The call is already being monitored by someone else.
- The call you are trying to monitor is on a phone that does not have a built-in bridge, or the built-in bridge has not been turned on in Unified CM Administration.

Action. If the call is already being monitored, wait and try to monitor the call at a later time. If there is a problem with the phone’s built-in bridge, turn on the built-in bridge in Unified CM, or replace the phone with a model that has a built-in bridge.

The live monitor request failed

Description. Due to a software error, this message is displayed instead of the actual error message, “The Unified CM rejected the request to silently monitor this extension.”

This error message appears when the extension is valid and is known to the Unified CM, but it is not configured correctly so you cannot monitor an agent. The extension might be incorrectly configured for one of the following reasons:

- The extension is not configured correctly in Unified CM.
- The extension is not part of the JTAPI application user.
- The extension is not in the correct monitor calling search space.
- The JTAPI application user does not have Live Monitoring privileges.

Action. Make sure that the supervisor extension is part of the JTAPI user and has a calling search space for the extension that includes the agent line or device partition to allow monitoring the agent.

Recording Monitoring Error Messages

Desktop client not connected

Description. The desktop client is not connected.

Action. Verify that the desktop client is connected and try again.

Device extension not valid

Description. The extension for the device is not valid.

Action. Correct the extension and try again.

Device MAC address not valid

Description. The MAC address for the device is not valid.

Action. Correct the MAC address and try again.

N/A

Description. There is no recording error associated with this agent.

Action. None.

No clients connected to receive events

Description. No clients are connected to the Load-balancing Subscription service to receive events.

Action. Verify clients are connected to the Load-balancing Subscription service and try again.

No proxy ID

Description. There is no proxy ID.

Action. Verify that there is a proxy ID and try again.

No SIP invite

Description. No SIP invite is sent to the Network Recording service to initiate a recording.

Action. Contact your Cisco Unified CM administrator to verify the Cisco Unified CM configuration.

No workflow has been defined for this user

Description. The user is not associated with a workflow.

Action. Assign the user to a team or a group that is associated with a workflow and try again.

Recording empty

Description. The recording file is empty (1kb).

Action. This indicates RTP was not delivered to the PC from the phone. Verify the phone configuration. Make a test call to ensure the .raw files are growing in size during the call.

Server capacity reached

Description. The Voice Record server reached its maximum capacity for recordings.

Action. Free up space on the Voice Record server.

Server free disk threshold reached

Description. The server has run out of hard drive space and recording stops until more free space becomes available.

Action. Remove unnecessary files from the Record Server or move files to a backup location.

Screen recording failed

Description. The Desktop Recording service failed to start recording.

Action. Restart the Desktop Recording service; Quality Management initializes the screen device. Verify the Screen Playback Gateway (PROXY Pro Gateway) service is running. If the Screen Playback Gateway service is not running, restart the Screen Playback Gateway (PROXY Pro Gateway) service.

Screen recording failed - stop

Description. The screen recording failed to stop.

Action. Restart the Desktop Recording service; Quality Management initializes the screen device. Verify the Screen Playback Gateway (PROXY Pro Gateway) service is running. If the Screen Playback Gateway service is not running, restart the Screen Playback Gateway (PROXY Pro Gateway) service.

Screen recording not responding

Description. The Desktop Recording service is not responding.

Action. Restart the Desktop Recording service; Quality Management initializes the screen device. Verify the Screen Playback Gateway (PROXY Pro Gateway) service is running. If the Screen Playback Gateway service is not running, restart the Screen Playback Gateway (PROXY Pro Gateway) service.

Screen Recording Successful

Description. The screen recording completed successfully.

Action. None.

Unknown failure

Description. An unexpected failure has occurred.

Action. Contact your system administrator.

Unknown screen failure

Description. An unexpected failure has occurred during screen recording.

Action. Contact your system administrator.

Unknown voice failure

Description. An unexpected failure has occurred during voice recording.

Action. Contact your system administrator.

User has no team

Description. The user is not associated with a team.

Action. Assign the user to a team in Monitoring and Recording Administrator Quality Management Administrator and try again.

User not licensed

Description. The user is not assigned to a license.

Action. Assign the user to a license in Monitoring and Recording Administrator Quality Management Administrator and try again.

Voice recording did not close normally

Description. The voice recording did not end normally.

Action. None.

Voice recording failed to start

Description. Voice device failed to start recording.

Action. Restart the Desktop Recording service; Quality Management initializes the voice device.

Voice recording failed to stop

Description. Voice device failed to stop recording.

Action. Restart the Desktop Recording service; Quality Management initializes the voice device.

Voice recording failing to find packets

Description. No packets were received for at least the first 15 seconds of the recording.

Action. The following device settings are required for desktop monitoring to function correctly in Quality Management.

> **NOTE:** Not all devices or Unified CM versions use all these settings. Configure those that do appear for your device and Unified CM version.

In Unified CM Administration, in the Product Specific Configuration section of the Device Configuration screen, configure these settings:

- PC Port—Enabled. If the PC Port is disabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.
- PC Voice VLAN Access—Enabled. If the PC Voice VLAN Access is disabled, no voice steams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.
- Span to PC Port—Enabled. If the Span to PC Port is disabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

In the Device Information section of the Device Configuration screen, configure this setting as follows:

- Device Security Mode—Non-Secure or Authenticated. If the Device Security Mode is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

You must also configure the agent phones to use the G.711 or G.729 codecs. Other codecs, such as G.722, are not supported for silent monitoring and recording.

Voice recording not allowed

Description. The extension for the device is not part of the Inclusion List.

Action. Add the extension to the Inclusion List and try again.

Voice recording successful

Description. The voice recording completed successfully.

Action. None.

Wrong user license

Description. The user has a Calabrio MediaSense License but is not configured to record through Calabrio MediaSense.

Action. Change the user's license type or configure the user to record through Calabrio MediaSense.

Audit Trail Error Messages

This topic describes the audit trail error messages that can appear in the User Recording Status and System Status reports generated through Cisco Unified Workforce Optimization.

Miscellaneous Informational Messages

Extensions changed: <extension numbers>

Description. The extension numbers for the logged-in user have changed.

Action. None.

Logged in with version: <current version>.

Description. A Quality Management user logged into their machine. The Quality Management user's machine is running the specified version of Desktop Recording service.

Action. None.

Current client version: <current version>.

Description. The Quality Management user's machine is running the current version of the client application.

Action. None.

Uploaded (voice): <ID>.

Description. A voice recording was uploaded.

Action. None.

Logged out.

Description. A Quality Management user has logged out.

Action. None.

Event Messages

Client heartbeat has stopped.

Description. Socket communications between the client and Quality Management server stopped.

Action. None.

Wrong client version: <current version>.

Description. The Desktop Recording service is not running the current version.

Action. Uninstall the old Desktop Recording services, and then install the current version of the Desktop Recording service.

Workflow Messages

This user does not have an assigned workflow and is not configured for archiving. No recordings will be made.

Description. The user is not assigned to a quality management workflow or an archive workflow. As a result, no recordings will be made for this user.

Action. Assign the user to a workflow if you want this user's calls to be recorded.

This user has only compliance licensing with no archive workflow. No recordings will be made.

Description. The user has a Compliance Recording license, but is not assigned to an archive workflow. As a result, no recordings will be made for this user.

Action. Assign the user to an archive workflow if you want this user's calls to be recorded.

Recording Messages

The audit trail messages for recording issues are as follows.

Common Recording Messages

Recorded (voice): <number of voice files>

Description. The number of recorded voice files ready to be uploaded.

Action. None.

Recorded (voice/screen): <number of voice and screen files>

Description. The number of recorded voice and screen files ready to be uploaded.

Action. None.

Uploaded (voice/screen): <number of voice and screen files>

Description. This message specifies the number of uploaded voice and screen files.

Action. None.

QM recording software is ready to record

Description. The Desktop Recording service is ready to record.

Action. None.

At least one required component for screen recording is not running

Description. A component required to record the screen is either not running or not installed.

Action. In the Windows Services utility in Control Panel, verify that the Screen Playback Gateway (PROXY Pro Gateway) service is installed and running. If the Screen Playback Gateway service is not present or unable to start, remove the Desktop Recording service, and then reinstall the Desktop Recording service.

Conversion from raw to spx failed

Description. Failed to convert the voice file from *.raw to *spx format. This might indicate that no RTP was delivered at the time of the recording.

Action. Try one of the following actions.

- If you are using Desktop or Network Recording, check the phone configuration.
- If you are using Server Recording (SPAN), check the SPAN.

Extension number(s) is/are not in the inclusion list: <extension numbers>

Description. The extensions from the agent's phone are not in the inclusion list. Quality Management does not record calls.

Action. Add the extensions you want to record to the inclusion list.

Screen recording failed to start

Description. The Desktop Recording service failed to start recording.

Action. Restart the Desktop Recording service; Quality Management will initialize the screen device. Verify the Screen Playback Gateway (PROXY Pro Gateway) service is running. Restart the Screen Playback Gateway service.

Screen recording not responding

Description. The Desktop Recording service is not responding.

Action. Restart the Desktop Recording service; Quality Management initializes the screen device. Verify the Screen Playback Gateway (PROXY Pro Gateway) service is running. If the Screen Playback Gateway service is not running, restart the Screen Playback Gateway (PROXY Pro Gateway) service.

Service is stopped while user has not logged out: <user name>

Description. The Desktop Recording service stopped while the user is still logged in. Quality Management does not record calls.

Action. Restart the Desktop Recording service or reboot the computer.

This user must belong to a team to record: <domain\username>

Description. The specified user does not belong to a team. Quality Management does not record calls.

Action. Assign the user to an ACD or Quality Management team and synchronize the data with Quality Management using Quality Management Administrator to initiate the synchronization process. For quality management recording, verify the team is assigned to a workflow.

Unable to retrieve phone information

Description. The Desktop Recording service was unable to detect the MAC address for the connected phone. Quality Management does not record calls.

Action. Verify the agent's phone and computer are connected in accordance with the section, "Desktop Recording (Endpoint) Service Requirements" in the *Installation Guide*. If Quality Management no longer detects the phone, Quality Management sends a message through MANA.

If the agent's phone and computer are connected correctly and the problem still exists, try the following.

- Update the user's NIC driver.
- Run a Wireshark capture to verify that the phone is communicating properly with the client PC. Filter the capture for SKINNY (or SIP in the case of a SIP phone) to verify the phone is forwarding its traffic to the client PC.
- Verify there is no security software or virus checking software that is blocking the Voice VLAN traffic from the phone.

Uploaded (voice): <number of voice files>

Description. This message specifies the number of uploaded voice files.

Action. None.

User is not configured to record: <user name>

Description. The user is logged into Cisco Unified Workforce Optimization but cannot record calls. You must configure the user to record calls in Quality Management Administrator.

Action. Use Quality Management Administrator to configure the user to record calls.

User is not licensed to record: <user name>

Description. The user is logged into Cisco Unified Workforce Optimization but cannot record calls. You must license the user to record calls in Quality Management Administrator.

Action. Use Quality Management Administrator to license the user. Then tell the user to log out and then log back in to begin recording.

Voice recording failed to start

Description. Voice device failed to start recording.

Action. Restart the Desktop Recording service; Quality Management initializes the voice device.

Zero byte file uploaded: <file name>

Description. The size of the uploaded file is zero.

Action. This indicates RTP was not delivered to the PC from the phone. Verify the phone configuration. Make a test call to ensure the .raw files are growing in size during the call.

Calls are not being recorded for devices that are not configured in QM for network recording: <device name>

Description. A device is not configured in Quality Management Administrator for Server Recording (SPAN) or Network Recording, so calls are not being recorded for that device.

Action. Make sure the device is configured in Unified CM and Quality Management Administrator.

Not enough free disk space to continue recording: <path> <remaining free space>

Description. Recording stops until more free space becomes available.

Action. Remove unnecessary files or move files to a backup location.

Calls are being recorded for a device that is not configured for this record server: <device name>

Description. The expected Server Recording server or Network Recording server is not recording calls for the device. Another Record Server is recording calls for the device. This is a possible failover situation.

Action. Verify the configuration is correct. Ensure the Server Recording server or Network Recording server is up and running.

The maximum number of concurrent recordings was reached on Quality Management Record Server

Description. The concurrent recordings on the Quality Management Server Recording server Network Recording server reached the maximum amount configured for the server.

Action. Add a new Server Recording Server or Network Recording server.

Approaching the maximum number of concurrent recordings on Quality Management Record Server: <number of concurrent recordings>/<maximum number of concurrent recordings>

Description. The concurrent recordings on the Quality Management Server Recording server or Network Recording server is approaching the maximum amount configured for the server.

Action. Consider adding a new Server Recording server or Network Recording server.

Free disk space is approaching the threshold where recording will stop: <path> <remaining free space>

Description. Free disk space is approaching the minimum amount of free disk space required. When the amount of free disk space reaches the minimum required, recording will stop.

Action. Remove unnecessary files or move files to backup location.

Prior free disk space warning canceled: <path> <remaining free space>

Description. More disk space is now available. Therefore, the previous disk space warning is canceled.

Action. None.

CCM detected is not configured in QM: <CCM>

Description. The Unified CM associated with this phone is not configured in Quality Management.

Action. To use this phone, configure Quality Management to support the Unified CM associated with this phone.

Recording Messages for Unified CCX

No packets were received for at least the first 15 seconds of the call: <device name>

Description. When you are monitoring an agent's customer contact, you can hear nothing. After 15 seconds, an error message indicates no packets are being received. Your attempt to record the agent's customer contact results in an empty recording. The agent's desktop is monitored using desktop monitoring.

Action. The following device settings are required for desktop monitoring to function correctly in Quality Management.

> **NOTE:** Not all devices or Unified CM versions use all these settings. Configure those that do appear for your device and Unified CM version.

In Unified CM Administration, in the Product Specific Configuration section of the Device Configuration screen, configure these settings:

- PC Port—Enabled. If the PC Port is disabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.
- PC Voice VLAN Access—Enabled. If the PC Voice VLAN Access is disabled, no voice steams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.
- Span to PC Port—Enabled. If the Span to PC Port is disabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

In the Device Information section of the Device Configuration screen, configure this setting as follows:

- Device Security Mode—Non-Secure or Authenticated. If the Device Security Mode is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

You must also configure the agent phones to use the G.711 or G.729 codecs. Other codecs, such as G.722, are not supported for silent monitoring and recording.

Recording CTI Service Messages

QM CTI service is connected: <CTI Server IP address>

Description. The Desktop Recording service is connected to the Quality Management CTI service.

Action. None.

QM CTI service is disconnected: <CTI Server IP address>

Description. The Desktop Recording service is not connected to the Quality Management CTI service. Quality Management does not record calls.

Action. Verify the Quality Management CTI server IP address is set correctly in Quality Management Administrator and that the Quality Management CTI service is running. Verify the JTAPI user name and password are correct for the configured Quality Management JTAPI user.

Free Space Messages

Free Space <path, current (Mb)>.

Description. Free space checks should occur periodically. The default configuration checks every 18 seconds when free space is less than or equal to 32000 Mb, and every 10 minutes when free space is greater than 32000 Mb. Before uploading a file, free space must be greater than or equal to the file size plus 90% of the failure threshold. The default failure threshold is 1000 Mb. FTS uploads also write to the Quality Management database EventAudit table. FTS has hardcoded warning thresholds of 32000, 16000, 8000, and 4000 Mb. Each time the amount of free space breaches the warning threshold, Quality Management writes the appropriate message to the EventAudit table and to the fts.log file.

Action. None.

Free Space: Checking free space failed. Free space checking has been disabled.

Description. At the startup of the Quality Management Jetty service on the Site Upload Servers, if FTS is unable to run the free space check, it turns off future free space checks.

Action. Troubleshoot why FTS was unable to run the free space check.

Free Space: Prior Warning Canceled. <path, current (Mb)>.

Description. A prior free space warning has been canceled.

Action. None.

Uploads Stopped: Not enough free space <path>.

Description. FTS has stopped uploading recordings to <path> because the location at <path> is full.

Action. Choose one of the following options:

- Add more storage.
- Remove unnecessary files.
- Move files to a backup location.

JTAPI Messages

The audit trail messages for JTAPI issues are as follows.

MAC address is not associated with the JTAPI user: <MAC address>.

Description. The MAC address for the agent's phone is not associated with the JTAPI user. Quality Management does not record calls.

Action. Be sure to correctly configure the phone in Cisco Unified CM. Verify the agent's phone is associated with the Quality Management JTAPI user. If you are using IP communicator, verify that the IP Communicator phone is configured using the MAC address of the user's PC, and that the MAC address is associated with the Quality Management JTAPI User.

Metadata Messages

The audit trail messages for metadata issues are as follows.

Failure to update metadata record due to invalid value for this metadata type <key>:<value>:<key>, <invalid value>

Description. The values in the metadata are not in the correct format.

Action. Ensure that the agent/metadata tool is putting the date and/or number values in the correct format. See the *Administrator User Guide* for valid formats.

Failure to update metadata record due to invalid key <key>:<invalid key>

Description. The metadata tool is not using the correct key as defined in Quality Management Administrator.

Action. Verify the metadata tool or the agent (if metadata tool or agent enters the key) uses the correct key as defined in Quality Management Administrator.

Troubleshooting Issues

Use the information presented here to diagnose and resolve problems.

Installation Issues

Use the information presented here to diagnose and resolve installation problems.

Cannot download client applications

Description. The client applications do not download when you click the links on the installation web page.

Symptom. When you click the install program link, an "HTTP 404—File Not Found" error appears.

Cause. System Configuration Setup did not complete successfully on the Quality Management Base Services server.

Solution. On the Quality Management Base Services server, navigate to the C:\Program Files\Cisco\WFO_QM\bin folder and double-click PostInstall.exe to launch the System Configuration Setup utility.

If the Tools menu is inactive, System Configuration Setup is running in Initial mode, and indicates it did not run to completion. If this occurs, navigate to each window and verify that you entered all required data, and then click Finish.

If System Configuration Setup starts in Initial mode, it did not complete correctly. Go through each window and make sure that you entered all required data, and then click Finish.

If System Configuration Setup is running in Update mode, choose Tools > Generate Info for MSI Clients. This operation regenerates the client installation files in the default location. After the operation completes, try to install the client applications from the installation web pages again. If the problem persists, contact technical support.

Cannot install application while another installation is in progress

Description. The following message appears on a client desktop.

```
Error 1500. Another installation is in progress. You must
complete that installation before continuing with this
one.
```

Cause. This message can appear when a user attempts to manually upgrade the Desktop Recording service after Automatic Updating has already initiated an upgrade. Because the upgrade is running in silent mode the user may not be aware that it is running.

Solution. Wait five minutes to allow the automatic upgrade to complete. Then check the Add or Remove Programs utility in Control Panel for the version of the installed application. If the version is not correct, manually install the upgrade.

Screen Playback Gateway Administrator does not appear in the Start menu after installation

Description. The following path does not appear in the Start menu:

```
Start > All Programs > Proxy Networks > PROXY Pro Gateway
Administrator
```

Cause. If you uninstall Screen Playback Gateway (PROXY Pro Gateway) Administrator without rebooting the machine, and then reinstall Screen Playback Gateway Administrator, and then reboot the machine, Screen Playback Gateway Administrator does not appear in the Start menu.

Solution. To access Screen Playback Gateway Administrator, choose one of the following options:

- Go to C:\Program Files\Proxy Networks\PROXY Pro Gateway, and then double-click PGADMIN.MSC.
- Go to C:\Program Files\Cisco\WFO_QM\bin, double-click PostInstall.exe, and then choose Tools > Show Proxy Networks Administrator.

Port conflicts with the Jetty webserver

Description. If IIS or Microsoft SQL Server 2008 Reporting Services is installed on the Quality Management server, it will create a port conflict with the Jetty webserver.

Cause. Quality Management builds the database and starts the Data API service when you run System Configuration Setup (PostInstall.exe) in Initial Mode. If IIS or Microsoft SQL Server 2008 Reporting Services is installed, an error message appears when starting the Data API service stating that the Data API service cannot be started or

accessed because IIS or Microsoft SQL Server 2008 Reporting Services controls the Jetty port.

Solution. Check Microsoft Windows Services to see if IIS or Microsoft SQL Server 2008 Reporting Services is installed and running. If IIS or Microsoft SQL Server 2008 Reporting Services is installed, disable it. Verify the Jetty service is running, and then restart System Configuration Setup.

Quality Management fails to connect to Microsoft SQL

Description. When first installed, Quality Management fails to connect to Microsoft SQL when building the database for Microsoft SQL Server 2008 SR2.

Symptom. The “Network error IOException: Connection refused: connect” message appears.

Cause. The TCP/IP protocol in SQL Server Configuration Manager is disabled.

Solution. Open SQL Server Configuration Manage, locate Protocols for MSSQLSERVER and enable TCP/IP.

Upgrade Issues

This topic explains how to diagnose and resolve problems that occur during upgrade.

Silent install of Desktop Recording Service reboots PC without notification after upgrade is complete

Description. If a client desktop is upgraded using the automated update feature, and if the Desktop Recording service is the application that initiates the automatic update, the client desktop will reboot without notification to the user. If either Quality Management Administrator or Cisco Unified Workforce Optimization is the application that initiates the automatic update, then the user will receive notification of a required reboot. Depending on the number of client desktops being upgraded simultaneously, system configuration, and the number of applications being upgraded, the reboot can occur up to 30 minutes after the upgrade process is initiated.

Symptom. The client desktop reboots without notification after the Desktop Recording service is upgraded via the automated update feature.

Solution. To avoid reboot without notification, disable the automated update feature and upgrade the desktop clients manually.

The screen portion of a recording does not play back after an upgrade.

Description. After you upgrade Quality Management, the screen portion of recordings do not play back.

Symptom. Screen recordings do not play back, while audio recordings do play back.

Solution. The client desktop browser cache is not cleared after the upgrade. This occurs with the applet because after the upgrade, the server has newer jar files than those cached on the user's desktop. To correct the problem, clear the browser cache and the Java cache.

To clear the browser cache: In Microsoft Internet Explorer, choose Tools > Internet Options > Delete Browsing History. Select the Temporary Internet files and Cookies check boxes, and then click Delete.

To clear the Java cache: Open the Windows Control Panel. Double-click Java to open the Java Control Panel. In the Temporary Internet Files section, click Settings, and then click Delete Files. In the resulting dialog box ensure that both check boxes are selected, and then click OK. It might take several minutes to clear the Java cache.

After you have cleared both the browser and Java cache, restart your browser.

Screen Playback Gateway fails to upgrade when launched by System Configuration Setup

Description. The Screen Playback Gateway installation fails in the following situations:

- You are moving from external storage to local storage
- You are moving from local storage to external storage
- The username and/or password changed for external storage
- You are upgrading Quality Management and you receive the error, "Error installing Proxy Gateway." This means that the Gateway.msi has failed.

Solution. Uninstall Screen Playback Gateway (PROXY Pro Gateway), and then run System Configuration Setup to reinstall Screen Playback Gateway.

1. Using the Windows Add or Remove Programs utility, uninstall PROXY Pro Gateway.
2. Restart the server.
3. If the PROXY Pro Gateway service is still listed in the Windows Services Control Manager, do the following:
    a. Stop the PROXY Pro Gateway service.

b. Open a command window and enter the following text to delete the service from the Windows Service control Manager: sc.exe delete ProxyGatewayService

4. Delete the following folders:
   - C:/Program Files/Proxy Networks
   - C:/Program Files/Common Files/Funk Software
5. Delete the following Windows registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.
6. Rerun System Configuration Setup.

A schema error appears when upgrading from 2.x to 9.0

Description. System Configuration Setup (PostInstall.exe) might fail when upgrading from 2.x to 9.0.

Symptom. The following error message appears.

```
Person_realmFK_skillTargetID_Unique is dependent on
column skillTargetID.
```

Solution. Modify skillTargetID in the SQMDB database.

1. Choose Start > All Programs > Microsoft SQL Server <year> > SQL Server Management Studio.

   The Microsoft SQL Server Management Studio window appears.
2. Type your authentication information in the fields, and then click Connect.
3. Expand the Databases node, and then click SQMDB.
4. Double-click Tables, right click Person, and choose Modify.

   The Table - dbo.Person tab appears.
5. Clear the Allow Nulls check box for skillTargetID, and then save your changes.
6. Rerun System Configuration Setup.

System Configuration Setup Issues

This topic explains how to diagnose and resolve problems that occur when running the System Configuration Setup tool (PostInstall.exe).

Historical data is lost

Description. User cannot find historical data for Quality Management.

Symptom. Historical data that was present is no longer in Quality Management.

Cause. The location of the Enterprise database was changed through System Configuration Setup (PostInstall.exe). All information that was contained in that database is no longer available for Quality Management to access.

Solution. Restore the original settings in the Cisco Unified CC Database window in Quality Management System Configuration Setup. If problems persist, contact technical support.

A Linux server name containing hyphens breaks the ODBC connection

Description. User entered the Linux server name in the Server Name field on the Cisco Unified CC Database window. The Linux server name contained one or more hyphens (for example, linux-ccx-server).

Symptom. The Linux server name broke the ODBC connection.

Solution. Replace each hyphen in the server name with an underscore when you enter the server name in the System Configuration Setup utility. This ensures the correct configuration of the file name.

JTAPI Issues

This topic explains how to diagnose and resolve JTAPI problems.

DNIS appears as “Conference”

Description. Quality Management uses JTAPI for call events. The Calling Number shown in Cisco Unified Workforce Optimization is the unmodified calling number. It will stay the same throughout the call, no matter if the call is transferred or conferenced. The Called Number shown in Cisco Unified Workforce Optimization is the last route point it went through. If the call was a direct call (or the route points are not being monitored by the JTAPI user defined in Site Configuration in Quality Management Administrator) it will be the unmodified calling number. It will stay the same through transfers and conferences.

Symptom. In a conference call, the DNIS appears as “Conference.”

Solution. There might be cases where the unmodified calling/called number is unknown due to devices being registered while the call is already in progress. Refer to the JTAPI Guide for your version of Unified CM.

Call Detail Record

This topic explains how to diagnose and resolve problems that occur with the Call Detail Record (CDR).

CDR does not report any missed calls when it should

Description. A call that matches the Do Not Record classifier might be reported as a missed call in CDR if it matches subsequent classifiers. The Do Not Record Classifier is ignored by CDR notifications.

Solution. None.

Recording Issues

This topic explains how to diagnose and resolve problems that occur with contact recordings.

Common Recording Issues

Recording is associated with the wrong agent and might be missing the beginning or end of the recording

Symptom. A recording is associated with Supervisor or Manager X, but the actual recording is for a call handled by Agent Y. Additionally, the beginning or end of the call is missing.

Cause. If a supervisor or manager is configured to record, and live-monitors an agent's call, the Live Monitoring session is recorded.

Solution. You can avoid this situation by configuring a second extension on the supervisor's or manager's phone and adding it to the exclusion list. See the *Administrator User Guide* for more details on configuring the exclusion list.

Parts of translucent windows do not appear in screen recording

Description. The desktop being recorded is running Vista with the Aero Glass Windows theme (translucent windows).

Symptom. Translucent windows, such as WebEx windows, are not captured.

Solution. A registry key was added to prevent screen flicker in Vista systems. This registry key also prevents translucent windows from being captured. To allow screen capture of translucent windows, remove the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\Proxy v5\TransparentWindows.....0 (0x0000).

Screen recording fails on the second call

Description. On an interleaved call, the screen recording on the second call results in a 1K file. The screen recording portion is not captured.

Symptom. A 1K file appears for the screen recording of the second call in an interleaved call scenario.

Solution. None.

When playing back a recording, the voice portion plays but the screen portion does not

Description. Media Player plays back only the voice portion of a recording.

Symptom. When you try to play back a recording, the following error message appears:

```
Error while connecting to screen server. Media Player
plays the voice recording without the screen recording.
```

Solution. To correct this problem, do the following:

1. On the Site Upload Server, uninstall Screen Playback Gateway (PROXY Pro Gateway) using the Add or Remove Programs utility.
2. On the Site Upload Server, start System Configuration Setup (PostInstall.exe).
3. Choose Tools > Set Recording Home Directory.
4. In the Recording File Storage Location dialog box, select the External Storage Location option in the Voice Recordings section. In the Storage Location field, enter the UNC path to the location where recordings are to be stored.
5. In the Screen Recordings section, select the Use same path as voice recordings check box.
6. In the Logon User section, enter the username and password of a user who has administrator rights on the Record Server.
7. Click OK. System Configuration Setup reinstalls Screen Playback Gateway and sets it to run as the administrator.

Desktop recording fails

Symptom. No recording files are in the C:\Program Files\Common\QM\Recordings folder on the desktop where recording is failing.

Solution. Check the following list for possible causes and solutions:

- Verify that the DNS is configured to resolve IP addresses and host names. From the PC where desktop recording is failing, run the command ping `-a <Unified CM IP address>`. If the ping cannot resolve the IP address, then neither can the Desktop Recording service. Configure the DNS so that host names and IP addresses are resolved.
- Verify that the Desktop Recording service is running.
- Verify that the phone and PC is correctly daisy-chained. You must directly connect the IP phone to the Ethernet jack. Connect the PC to the phone's PC port. Enable the phone's PC port.
- Verify that the client PC is connecting to SQL database. The DesktopRecordServer.dbg has a statement should contain the following statement:

  ```
  Connected to service at <Quality Management SQL server IP address>.
  ```

- Verify that you entered the correct information for Unified CM in the Cisco Unified CM or window of the System Configuration Setup tool.
- Verify the following messages appear:
  - In the ctiservice.dbg log—MAC not in domain. <MAC address>.com.calabrio.sqm.ctiservice.CtiException: Specified MAC not in domain: <MAC address>.
  - In the DesktopRecordServer.dbg on the agent's PC—The MAC address <phone's MAC address> is not associated with the JTAPI user.
- Verify that you connected the Quality Management CTI service to the Unified CM CTI Manger by looking in cti.dbg for the following message:

  ```
  SQM CTI Service ready.
  ```

- Verify that the phone is configured in Unified CM according to the *Installation Guide*.

Action. If the phone is configured correctly and the problem still exists, try the following.

- Use a packet capture tool (for example, Wireshark) to verify that the phone is forwarding RTP and phone protocol (SCCP or SIP) traffic to the NIC card on the client PC.
- Verify the Inclusion List node under Site Configuration in Quality Management is configured correctly. See the *Administrator User Guide* for more information.

Desktop Recording service fails to start on reboot in rare instances

Description. The Desktop Recording service might fail start after a reboot for the following reasons:

- User logs in over Virtual Private Network (VPN) and there is a delay in the startup time.
- Some computers, especially older systems, have slow startup times.
- The computer uses a large startup script that requires time to start up.

The Desktop Recording service has a dependency on System Event Notifications which delays the startup attempt. On some computers this dependency occurs before some long running task that prevents the Desktop Recording service from starting. For example, a computer might require over 10 minutes for startup and Service Control Manager does not start the Desktop Recording service.

Solution. Make sure the computer starts up quickly (under ten minutes). If your computer requires more than 10 minutes to startup, add a dependency for the Desktop Recording Service to start after a service that is common to every login script for your site. More information on delaying the loading of specific services is available at the following website:

http://support.microsoft.com/?kbid=193888

Screen recording playback fails when storage folder is in the wrong location

Description. Screen recording playback fails when the storage folder is in the wrong location. Voice recordings are unaffected. The system suffered a power failure but restarted successfully.

Solution. The path of the video folder on the Screen server changed to an incorrect location. For example, System Configuration Setup displays the screen recording storage path as C:\Program Files\Common Files\QM\recordings\video when they are actually located at E:\Program Files\Common Files\QM\recordings\video. Correct the folder path to the true location in System Configuration Setup and screen recordings will play back. If you configured the path correctly and the problem still exists, try the following.

- Stop, and then start the Screen Recording (PROXY Pro Recording) service on the Quality Management server.
- Map a drive to the recording storage location from the client running Desktop Recording service. If this fails, there might be a policy restriction on the user's Windows account.

Conversion from raw to spx failed

Description. The message, "Conversion from raw to spx failed" appears multiple times in the System Status report, but all the recordings for the specified agent for that day were uploaded correctly.

Solution. If the staging process that occurs after the configured End Of Day is interrupted before it completes, you might see this error message in the System Status report.

Part of the staging process involves converting the *.raw files to *.spx files. If the staging process is interrupted after some files have been converted and the *.raw files have been deleted, when the staging process resumes, it starts from the beginning so that it appears to fail converting the files that it already processed correctly before the interruption.

Examples of interruption include rebooting the PC or restarting the Desktop Recording service during the staging process. In these scenarios, no recordings are lost.

Audio and video streams are out of sync

Description. When playing a contact recording for evaluation, audio and video streams are out of sync.

Solution. Stop and then restart the playback to resync the audio and video. If that does not work, click the Cancel button and exit the evaluation form, then open it again and start over.

Network Recording service stopped

Description. The Network Recording service stopped while an agent is on a call, and then restarted before the call ends. The call recording only goes until the Network Recording service stops. It does not include time through end-of-call.

Solution. When the Network Recording service stops, it drops the connection to the Recording CTI service, which in turn drops the connection to JTAPI. The Recording CTI service discards all history associated with that client.

When a new connection is established, the JTAPI provides a snapshot of call events (ringing, established, and so on), but does not include RTP events. In the case of the Desktop Recording service (the endpoint recording client), it begins to record again since that service uses only call events. However, the Network Recording service (SPAN and Network Recording) requires RTP events to begin recording. It starts recording on the next RTP event (this could be after a hold on the same call).

Screen recording prompts for a username and password

Description. When you play back a screen recording, Quality Management displays a Login dialog box. This typically happens when using external screen storage.

Solution. On the screen server:

1. Launch Screen Playback Gateway Administrator (Start > Programs > Proxy Networks > PROXY Pro Gateway Administrator).
2. Navigate to Gateway Security.
3. In the right pane, click the link, Click here to Change Operation Security.
4. On the Operation Security tab, select the Connect to File check box.

No export files are generated

Description. No export files are generated when using the Server API exportRecording operation to perform server-based exporting.

Solution. Try the following solutions.

- Restart the Jetty Service.
- Use Cisco Unified Workforce Optimization to export recordings to wave or wmv files.

If the problem persists, contact technical support. For more information, see the *Administrator User Guide*.

Contact recordings are not uploaded

Description. Quality Management is not uploading contact recordings.

Symptom. When Quality Management does not upload contact recordings, look for the following symptoms.

- The start time is off by an hour. This can happen when a time zone changes its rules (for example, DST is changed to another date and/or time).
- The dbproxy.log contains the following message.

  Unknown Java Timezone ID: null. Endpoint Timezone

Cause. Unable to update time zone in the data because the time zone is not in the tzmappings file (for example, Pakistan Standard Time). The Java version shipped with Quality Management does not include the Windows time zone specified in the dbproxy.log.

If the problem persists, contact customer support.

Solution. To update the tz database for Java to include your time zone:

1. Go to the following website:

   http://www.oracle.com/technetwork/java/javase/downloads/index.htm
2. Scroll down to JDK DST Timezone Update Tool (tzupdater) and click Download.

The tool is bundled in a zip file.

3. Extract the files from the zip file to a known directory.

   You can choose to extract the file to the Java\bin folder.

   - If you installed Quality Management in the default location, the directory path is C:\Program Files\Cisco\WFO_QM\Java\bin.
   - If you do not know where Quality Management is installed, the HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\QM\Site Setup\INSTALL DIRECTORY in the Windows registry provides the installation location.

4. Select Start > Run, type `cmd` in the Open field, and then click OK.
5. Enter the following command.

   ```
   cd <directory path>
   ```

   Where <directory path> is the location of the Java\bin folder.
6. Enter the following command to check the current Java version against the downloaded tzupdater.jar version.

   ```
   java -jar <known directory path>tzupdater.jar -V
   ```

   Where <known directory path> is the location of the tzupdater.jar file. If the tzupdater.jar is in the Java\bin directory, you do not need to specify the known directory path.

   NOTE: These commands are case sensitive.
7. Enter the following command to update the JRE's timezone version.

   ```
   java -jar <known directory path>tzupdater.jar -u
   ```
8. Enter the following command to verify the current Java version is the same as the downloaded tzupdater version.

   ```
   Java -jar <known directory path>tzupdater.jar -V
   ```

Archive call was tagged for quality, but is not visible in the Recordings application

Description. A call from today is viewable in the archive and tagged for quality. When you look for the call in the Recordings application, you cannot locate the call.

Symptom. Cannot find the call in the Recordings application.

Cause. The call has not yet been uploaded.

Solution. The call will be available in the Recordings application if you play the recording from the Archive, or after the End of Day upload has occurred.

If client desktop cannot connect to the server, contact recordings assigned to the quality management workflow fail to upload

Description. If the recordings belong to the quality management workflow and the client desktop cannot connect to the server, the recordings fail to appear in the Recordings application after End of Day.

Symptom. The files moved to the staging folder and uploaded to the server, but the recordings do not appear as quality recordings in the Recordings application. The contact recordings appear as archive recordings in the Recordings application.

Cause. Because the desktop client could not connect to the server, the files were marked for the archive workflow by default because the Quality Management Base Services server could not find an entry for the agent and verify the agent's workflow information.

Solution. Search for the archive recordings in the Recordings application and mark the contact recording for quality scoring. When you mark the contact recording for quality scoring, the contact appears as a quality recording in the Recordings application.

The Recording CTI service creates one huge recording file for all subsequent calls

Description. The Recording CTI service does not appear to be recording individual calls. All calls appear in one huge recording file.

Symptom. No recordings appear on the client desktop.

Cause. The Recording CTI service starts recording a call and does not end recording when the call ends. The recording continues through subsequent calls and appears like it is not recording. The recordings folder contains one large .raw file that continues to record all subsequent calls once this event triggers.

Solution. Restart the Recording CTI service.

Record Servers do not reconnect after restarting the Base server

Description. The Record Servers do not reconnect to the Quality Management Base server after you restart it.

Symptom. One or more Record Servers are not recording calls.

Cause. Restarting the Base server in a multiple record server environment can cause race conditions within the Record Servers as they disconnect and reconnect to the Base server. As a result, a Record Server might fail.

Solution. When restarting the Base server, perform the following task.

1. Schedule the Base server for maintenance when agents are not recording calls.
2. Stop the Network Recording service on all Record Servers.
3. Stop the Monitor service on all Monitor Servers.
4. From the Base server, choose Start, then select Restart from the Shut Down Windows dialog box, and click OK.
5. log in to the Base server and verify the services are running.

6. Start the Monitor service on all Monitor Servers.
7. Start the Network Recording services on all Record Servers.
8. Log in as a test user and record some calls. Repeat this test for each Record Server in your environment.
9. log in to Cisco Unified Workforce Optimization, and verify the recordings are available and playable.

Playing a recording fails

Description. A user cannot play a recording. This situation only applies to Network Recording configurations with a primary Record Server and a backup Record Server.

Symptom. An agent is configured for Network Recording on the primary backup server. If the primary Record Server fails, SIP messages are then sent to the backup Record Server and the agent's recordings are captured and stored on the backup Record Server. If the primary Record Server recovers and the backup Record Server fails or loses connectivity with the Upload Controller, the call information will not be sent to the Upload Controller. Download on Demand fails because the Upload Controller does not know about the calls received by the agent while the primary Record Server was down. Playing a recording fails because the Upload Controller does not know about the calls received by the agent when the agent was configured for the backup Record Server.

Cause. A recording failover occurred.

Solution. The recordings on these servers will not be available for playing until after they are uploaded to the Upload Controller.

Cannot play back screen recording when the Base server is Windows Server 2008 32-bits

Description. User cannot play back screen recording.

Symptom. Media Player is unable to connect to the Proxy Gateway to play back a screen recording. You can play back the voice recording but not the screen recording. Playing back a screen recording fails 100% of the time on some servers, but never on other servers. It appears to occur most often on Windows Server 2008, but not all instances of Windows Server 2008 32-bits.

Cause. This is a permissions issue. The root cause is unknown. Use the procedure documented in the "Running System Configuration Setup" of the *Installation Guide* to allow the Administrators group to Connect to File. The user (RemoteControlGateway) used to connect to the Gateway Administrator application is assigned to the Administrators group and that group has the correct permissions in the Gateway Administrator application.

Workaround. To resolve this issue, choose one of the following options.

- Add the RemoteControlGateway user to both the Data Service Security tab and the Operation Security tab in the Gateway Security application and choose the Allow check box next to Full Control/Administration. The Media Player can now connect to the Proxy Gateway and play back screen recordings.
- Manually uninstall the Screen Playback Gateway, start System Configuration Setup (C:\Program Files\Cisco\WFO_QM\bin\PostInstall.exe), and then choose Tools > Set Recording Home Directory. From The Recording File Storage Location window, type the Universal Naming Convention (UNC) path to the storage location (for example, \\10.10.51.83\C$\Program File\Common Files\QM\recordings), choose External Storage Location, type the administrator's login information in the Username and Password fields, and then click OK. System Configuration Setup reinstalls the Screen Playback Gateway and configures it to run as the administrator.

Voice and screen recordings are out of sync

Description. The voice and screen recordings are out of sync when you play back the recording.

Symptom. The audio might be slightly delayed when you play back a recording.

Cause. The SQM service stopped while a call was being recorded.

Solution. None.

Screen recording export fails when the operating system for the Base server is Windows Server 2008

Description. Desktop Experience must be installed on Windows Server 2008 if you are going to use it as a Quality Management Base server. Desktop Experience allows the end users to export screen recordings or WMA from the Cisco Unified Workforce Optimization interface.

Symptom. Export fails when you export a screen recording from a Base server that is running Windows Server 2008.

Cause. Desktop Experience was not installed on Windows Server 2008.

Solution. Install Desktop Experience on Windows Server 2008. The instructions are provided in the *Installation Guide*.

"Error writing Audit Trail" message appears when trying to open a contact

Description. The following message appeared when trying to play a contact recording:

```
QMREC2009 Error writing audit trail
```

Symptom. You cannot play back a contact recording.

Solution. Log out of Calabrio ONE, log in to Calabrio ONE, and then play the contact recording again.

Cannot hear the audio recording without clicking the progress bar on a contact recording

Description. When playing a contact recording, the voice recording is not audible until you click the progress bar (slider bar).

Symptom. There is no audio sound when playing a contact recording.

Solution. Click the progress bar or open the contact recording a second time to hear the audio recording.

Recording Issues for Cisco MediaSense

Calling Number displays UNKNOWN on a segment of a Calabrio MediaSense conference call.

Symptom. When you look at a Calabrio MediaSense recording for a conference call in the Recordings application, the Calling Number field displays UNKNOWN.

Cause. When the other participant in a segment of a Calabrio MediaSense recording is a conference bridge, the ANI and DNIS is unavailable and the Calling Number field displays UNKNOWN.

Solution. None.

MediaSense Subscription service lost connection to the Cisco MediaSense Record server

Symptom. The MediaSense Subscription service lost connection to the Cisco MediaSense Record server and cannot retrieve recordings.

Cause. The Calabrio MediaSense Subscription service lost connection to the Cisco MediaSense Record server

Solution. Once the connection from the MediaSense subscription service is reestablished to the MediaSense Record server, Quality Management will check for any calls to be retrieved during the outage every 10 minutes.

Recording Issues for Cisco Unified CCX

Calls for devices configured for Network Recording drop when you try to conference or transfer a call.

Symptom. When you try to transfer or conference a call and one or more devices on the call configured for Network Recording, the transfer or conference fails and parties drop off of the call.

Cause. Cisco Unified CM does not support codec changes for devices that are configured for call recording. The codec must remain the same throughout the life of the call. For conference calls, the conference bridge must support the codec used before the conference completes.

Solution. Update the Cisco Unified CM configuration to ensure that no codec changes occur for network recorded devices. See the Cisco Unified CM documentation for more information.

Calls for devices configured for Network Recording are not recorded.

Symptom. Calls for devices configured for Network Recording are not recorded. No raw files or 1K raw files appear in the recordings folder.

Cause. Possible causes are as follows:

- The device is not configured in Quality Management Administration for Network Recording.
- The extension is not configured in Cisco Unified CM for Network Recording. All extensions on the device that you want to record need to be configured for recording. In this instance, the Cisco Unified CM is not sending a SIP INVITE to the Quality Management Network Recording service to initiate a recording.
- The call is not using a supported codec. Supported codecs are G.711, G.722, and G.729.
- The SIP trunk for the recorder is not configured properly in Cisco Unified CM. The SIP trunk needs to point to the Quality Management Network Recording service IP address and port 5060.

Solution. Correct the misconfiguration based on the above possible causes.

Use a packet sniffer to check if the Cisco Unified CM is sending a SIP INVITE to the Quality Management Recording service. The Cisco Unified CM should send a SIP INVITE to recording-enabled extensions every time a call is answered or retrieved from a held state. SIP INVITE messages should be sent from a Cisco Unified CM IP address to the Quality Management Network Recording service server IP address on port 5060. The IP protocol used can be either UDP or TCP.

If no SIP INVITE messages appear, then engage the Cisco Unified CM administrator or support team to verify the Cisco Unified CM configuration.

In some cases, the Cisco Unified CM configuration might appear to be correct for the phone, yet no SIP INVITE messages are sent to the recorder. Deleting and recreating the phone in Cisco Unified CM might resolve the issue.

Recording drops 5–10 seconds of audio

Description. Recording drops 5–10 seconds of audio near the beginning of a call.

Symptom. When CAD and Quality Management are running on the same machine, the recording is missing audio near the beginning of a call and the recording quality might also be garbled.

Solution. Verify the DNS is configured to resolve host names of the CAD Record Servers. From the PC where desktop recording is failing, open a command window and enter ping -a <CAD Record Server hostname>. If the ping cannot resolve the CAD Record Server hostname, then neither can the Desktop Recording service. Configure the DNS so that host names are resolved.

Screen recording playback fails when CAD is installed on the client machine

Description. Playback of screen recording fails when CAD is installed on the client machine.

Solution.

- Stop, and then start the Screen Recording (PROXY Pro Recording) service on the Quality Management server.
- Map a drive to the recording storage location from the client running Desktop Recording service. If this fails, there might be a policy restriction on the user's Windows account.

Unable to record calls

Description. Unable to record calls from a SIP phone right after rebooting the PC.

Solution. To detect the connected IP phone, the Desktop Recording service monitors the heartbeat messages between the Unified CM and the IP phone. It may take up to 6 minutes after the Desktop Recording service starts to properly identify a SIP phone.

Screen recording fails

Description. Screen recording fails when using Server Recording (SPAN). This typically happens when using external screen storage.

Solution. On the screen server:

1. Launch Screen Playback Gateway Administrator (Start > Programs > Proxy Networks > PROXY Pro Gateway Administrator).
2. Expand the Local Gateway node, and then expand Gateway Server Settings.
3. Select Gateway Security.

4. In the right pane, click the link, Click here to change Operation Security.
5. On the Operation Security tab, select the Allow check box for the Record to File permission.

Garbled speech appears in the contact recording

Description. Garbled speech appears in the Quality Management contact recording when you use Cisco Unified CM-based monitoring.

Symptom. The garbled speech occurs when trying to silently monitor a conversation.

Cause. This type of silent monitoring sends an extra stream from the phone. The recording software for Quality Management, Desktop Recording (Endpoint), and Server Recording captures the extra stream and stores it in the call recording file. You can only use this type of silent monitoring with Cisco-supported hard phones.

Solution. Do not use this method of silent monitoring.

Calls continue to be recorded after Extension Mobility agents log out

Description. Calls continue to be recorded after Extension Mobility agent log out when the same extension is assigned to the device and the user profile.

Symptom. The call continues to be recorded after the agent logs out.

Cause. The same extension is assigned to the device and the user profile.

Solution. Do not assign the same extension to the device and the user profile.

Quality Management Administrator Issues

This topic explains how to diagnose and resolve problems that occur when running the Quality Management Administrator.

Common Quality Management Administrator Issues

Cannot log in to

Description. Administrator cannot log in to.

Symptom. The following message appears when the administrator tries to log in to:

```
Invalid login. Please try again.
```

Cause. This message might indicate one of the following issues:

- The password was entered incorrectly—enter the correct password.

- The password changed—ensure the user has the correct password
- There is an Active Directory issue—consult the Active Directory documentation to resolve this problem.

Solution. Reenter the login information and then try again. If the error persists, contact your administrator.

The administrator should check the following items to verify if the Windows account the user is logging in with is the correct account:

- Check the datapa.dbg file. If the username or password is invalid, the datapa.db file will contain the following error:

```
javax.naming.AuthenticationException: [LDAP: error code 49
- 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 525, vece
```

- Verify that you configured the Active Directory path correctly in Quality Management Administrator under Enterprise Settings.
- Verify the Quality Management server is in the user's domain, or in a trusted domain.
- Verify the administrator is included in the admin group in Active Directory. Administrators require this security setting if they are using Active Directory so that they can log into and Workforce Optimization. If the administrator is not in the admin group, the admin.dbg file will contain the following error:

```
"Caused by: 401 UNAUTHORIZED at
com.calabrio.qm.datapa.chap.QmAuthenticationHandler.authen
ticateAdUser(QmAuthenticationHandler.java:317)
```

  The name of admin group and the OUs that were searched for this group will appear under to "Searching for groupName:" immediately above the error.

  If the administrator is not in the correct admin group, perform the following steps:

  a. Verify the administrator is in the correct admin group in Active Directory.
  b. Verify the defined admin group exists within the provided domain.
  c. Verify the OUs defined for the domain can access the defined admin group.

Buttons appear cut in half

Description. On some windows in Quality Management Administrator (for instance, the questions area on the Evaluation Form Templates window), buttons appear cut in half.

Symptom. Buttons do not display correctly.

Cause. The Display DPI setting is set to something other than Normal.

Solution. In the Windows Control Panel, start the Display utility. On the Settings tab, click Advanced. In the resulting Plug and Play Monitor Properties dialog box, select the General tab and make sure the DPI setting is set to Normal size (96 dpi). Click OK twice to save and apply your settings.

Cannot find Active Directory users

Description. In Quality Management Administrator (Personnel > User Administration > Link Selected Users), you cannot find Active Directory users if the domain is identified by the host name.

Symptom. When you select a user, the Link Selected Users dialog box appears and displays domain information. However, when you click Find, an error message appears indicating that no data is available.

Cause. In Site Configuration, you added the Active Directory domains and the host name to identify the Active Directory connection. The connection was validated and the domain configuration was saved.

Solution. Edit the domain configuration to change the host name to an IP address. Once changed, Active Directory data can be found in the Link Selected Users window. If you want to continue using host names, add the host names to the DNS path to ensure that the host name is reachable by all computers.

Not enough calls are saved

Description. Not enough calls are saved for quality management workflows.

Symptom. Calls saved for quality management workflows only appear in the Recordings application in Cisco Unified Workforce Optimization when an agent shuts down or restarts their machine at the end of the day.

Solution. Either set the End of the Day time to a later time in Quality Management Administrator or ensure that the agent's machine does not shut down or restart at the end of the day.

Duplicate Sites

Description. If you create a site using the IP address (or hostname) and then change it to hostname (or IP address, Site Settings displays the same site twice.

Symptom. One tab displays the site's IP address and another tab displays the site's hostname.

Solution. Delete the duplicate site. Ensure the appropriate teams are assigned to the remaining site.

Quality Management Administrator Issues for

Sync service does not deactivate agents

Description. Sync service does not deactivate agents in Quality Management Administrator when you set an agent to inactive in Unified CM Administration.

Symptom. Agents who are inactive in Unified CM Administration appear as active in Quality Management Administrator.

Solution. If you do not want the inactive agent in Unified CM Administration to be able to log in to Cisco Unified Workforce Optimization or record contacts, you must unlicense the agent in Quality Management Administrator.

Changing a recording profile mid-call causes recording to stop working

Description. If you change the recording profile for a device in Cisco Unified CM from one server to another server while Quality Management is recording a call for that device, Quality Management stops recording the call.

Symptom. The recording ends abruptly.

Solution. Update the Record Server for the device in Quality Management Administrator, then wait 5 minutes or restart the Record Server.

Cisco Unified Workforce Optimization Issues

Use the information presented here to diagnose and resolve Cisco Unified Workforce Optimization problems.

There is a Problem with this Website's Security Certificate

Description. The following error message appears when you try to access the Cisco Unified Workforce Optimization interface using an https:// URL.

```
There is a problem with this website's security
certificate.
```

Cause. There is no certificate for this website.

Solution. To correct the problem, do the following:

1. Enter the following URL in your web browser, where <Base server> is either the IP address or the hostname of the Cisco Unified Workforce Optimization interface.

   ```
   https://<Base server>
   ```

where <Base server> is the IP address or hostname of the user interface.

2. When the error message appears, click Continue to this Website.
3. From Microsoft Internet Explorer, choose Tools > Internet Options, click the Security tab, select Trusted Sites, click Sites, click Add in the Trusted Sites dialog box, click close, and then click OK.
4. Click Certificate Error in the Address bar, click View Certificate, click Install Certificate in the Certificate dialog box, click Next, choose Place All Certificates in the following Store, click Browse, select Trusted Root Certification Authorities, click OK, click Next, and then click Finish.
5. Click Yes on the Security Warning dialog box, and then click OK.

A security warning appears when you click Validate my PC Configuration

Description. The following message appears when you click Validate my PC Configuration in Cisco Unified Workforce Optimization:

```
The application's digital signature cannot be verified. Do you
want to run the application?
```

Cause. The digital signature cannot be verified by a trusted source.

Solution. Click the Always Trust Content from this Publisher check box, and then click Run.

Cannot log in to Cisco Unified Workforce Optimization

Description. User cannot log in to Cisco Unified Workforce Optimization.

Symptom. The following message appears when the user tries to log in to Cisco Unified Workforce Optimization:

```
Credentials are not correct. Try again.
```

Cause: This message might indicate one of the following issues:

- The password was entered incorrectly—enter the correct password.
- The password changed—ensure the user has the correct password
- The user is unlicensed—assign a license to the user in to resolve this problem
- There is an Active Directory issue—consult the Active Directory documentation to resolve this problem.

Solution. Reenter the login information and then try again. If the error persists, contact your administrator.

The administrator should check the following items to verify if the Windows account the user is logging in with is the correct account:

- Check the DesktopRecordServer.dbg file for the credentials the user is using to log in.
- Verify that you configured the Active Directory path correctly in Quality Management Administrator under Enterprise Settings.
- Verify the Quality Management server is in the user's domain, or in a trusted domain.
- Verify the user is synchronized in Quality Management, linked, and licensed.
- Verify the user account in Quality Management was not deactivated and the agent was not removed from Unified CCX.
- If the user is an administrator, verify the administrator is included in the admin group in Active Directory. Administrators require this security setting if they are using Active Directory so that they can log into and Workforce Optimization. If the administrator is not in the admin group, the admin.dbg file will contain the following error:

```
"Caused by: 401 UNAUTHORIZED at
com.calabrio.qm.datapa.chap.QmAuthenticationHandler.authen
ticateAdUser(QmAuthenticationHandler.java:317)
```

  The name of admin group and the OUs that were searched for this group will appear under to "Searching for groupName:" immediately above the error.

  If the administrator is not in the correct admin group, perform the following steps:

  a. Verify the administrator is in the correct admin group in Active Directory.
  b. Verify the defined admin group exists within the provided domain.
  c. Verify the OUs defined for the domain can access the defined admin group.

Cannot log in to all products on Cisco Unified Workforce Optimization

Description. User tried to log in to multiple products on Cisco Unified Workforce Optimization, and partially succeeded in logging into only one of the products.

Symptom. If the information entered is incorrect for one of the products, the following message appears.

```
Credentials are not correct for <Product Name>. Click
Logout and try again.
```

Cause: This message might indicate one of the following issues:

- The password changed—ensure the user has the correct password

- The user is unlicensed—assign a license to the user in to resolve this problem
- There is an Active Directory issue—consult the Active Directory documentation to resolve this problem.

Solution. Reenter the login information and then try again. If the error persists, contact your administrator.

The administrator should check the following items to verify if the Windows account the user is logging in with is the correct account:

- Check the DesktopRecordServer.dbg file for the credentials the user is using to log in.
- Verify that you configured the Active Directory path correctly in Quality Management Administrator under Enterprise Settings.
- Verify the Quality Management server is in the user's domain, or in a trusted domain.
- Verify the user is synchronized in Quality Management, linked, and licensed.
- Verify the user account in Quality Management was not deactivated and the agent was not removed from Unified CCX.

Cannot access applications in Cisco Unified Workforce Optimization

Description. User cannot access applications in Cisco Unified Workforce Optimization.

Symptom. If the username and password are correct, but the user does not have permission to access the applications, the following message appears.

```
You do not have permission to access any Quality
Management applications. The Apps list is empty. Contact
your administrator to correct the problem.
```

Solution. Contact your administrator to correct the problem.

Reports do not open in Microsoft Internet Explorer 8 or 9

Description. Reports in CSV, PDF, and XLS format do not open in Microsoft Internet Explorer 8 or 9.

Symptom. A dialog box to save the report opens but closes again very quickly.

Solution. Choose one of the following solutions.

- Clear the Confirm open after download check box for the CSV, PDF, and XLS file types. To do this, follow these steps for each file type.

a. Double-click My Computer.
b. On the Tools menu, choose Folder Options.
c. Select the File Types tab.
d. Under Registered File Types, select the file type, and then click Advanced.
e. Clear the Confirm open after download check box, and then click OK.

NOTE: This solution might not work. In that case, try the following solution.

- Enable automatic prompting for downloads in Microsoft Internet Explorer.

a. In Microsoft Internet Explorer, choose Tools > Internet Options. The Internet Options dialog box appears.
b. Click the Security tab, and then click Custom level. The Security Settings - Internet Zone dialog box appears.
c. Scroll down to Downloads and click the Enable option for Automatic prompting for file downloads.
d. Click OK to save your changes.
e. Click OK to dismiss the Internet Options dialog box.

It takes 30 seconds to open Reporting after the server is booted

Description. The first person to access the Reporting application might have to wait up to 30 seconds for the Reporting application to respond after the server is booted.

Cause. When the server is booted, only the first person who accesses the Reporting application experiences this delay. Some time is required when the first user accesses the Reporting application. The Reporting application connects to the database, establishes privileges, and displays a menu based on the user's role. After the connection is established you can quickly access reports.

Solution. None.

A security warning appears when you click Recordings

Description. The following message appears when you click Recordings in Cisco Unified Workforce Optimization:

```
The application's digital signature cannot be verified. Do you
want to run the application?
```

Cause. The digital signature cannot be verified by a trusted source.

Solution. Click the Always Trust Content from this Publisher check box, and then click Run.

Agent cannot view quality management calls

Description. An agent cannot view quality management recordings for call, but can view archive recordings for calls in the Recordings application.

Cause. An agent cannot view calls when any of the following has occurred:

- The agent's team is not in a group.
- The agent is deleted from Unified CM.

Solution. To see the quality management calls in the Recordings application, do one of the following (as appropriate to the individual situation):

- Add the team to a group in Quality Management Administrator.
- Add the agent in Unified CM.

The error, "Can't move focus to the control because it is invisible, not enabled, or of a type that does not accept the focus" appears when choosing any menu item.

Description. This problem is due to a Microsoft Internet Explorer issue.

Solution. To prevent this error from appearing, edit the Microsoft Internet Explorer options as follows.

1. In Microsoft Internet Explorer, choose Tools > Internet Options, and select the Advanced tab.
2. Under the Browsing section, ensure that the "Display a notification about every script error" option is cleared; select the "Disable script debugging (Internet Explorer)" and "Disable script debugging (Other)" options.
3. Click OK.

Encrypted metadata appears as sortable in a table, but does not sort

Description. A sort triangle appears in a metadata column. When you click the sort triangle, the metadata in the column does not sort. The sort is ignored.

Solution. None.

The index for Japanese localized help does not display text in the correct sort order

Description. The text does not appear in the correct sort order in the Japanese localized help.

Solution. None.

Slow performance when the search filter locates many recordings

Description. If you use Search Recordings in Recordings application and the search filter locates many recordings, performance might be affected. A slow response to a search request can also affect the performance of other applications in the Cisco Unified Workforce Optimization.

Solution. Our testing has found that the time required to fully render a page within the Cisco Unified Workforce Optimization can vary from one web browser family to the next. If user interface performance is a major concern to your business practice, the web browsers perform page rendering in the following order from fastest to slowest:

- FF 3.x or later
- IE 9, 32-bit
- IE 8

Accented characters are garbled when you open a report in CSV format in MS Excel

Description. When you open a report containing accented characters in CSV format in Microsoft Excel, the accented characters are garbled.

Solution. Open the CSV report with Notepad.

Accented characters do not appear in PDF reports

Description. When you generate a report containing accented characters, the accented characters are missing from the PDF.

Solution. Run the report in HTML format.

Asian characters are garbled when you open a report in CSV format in MS Excel

Description. When you open a report containing Asian characters in CSV format in Microsoft Excel, the Asian characters are garbled.

Solution. Open the CSV report with Notepad.

Asian characters do not appear in PDF reports

Description. When you generate a report containing Asian characters, the Asian characters are missing from the PDF.

Solution. Run the report in HTML format.

Report does not correctly display data in locale language

Description. Data in a specific locale language does not appear correctly in a Quality Report when you generate a PDF form. The data appears correctly when you generate a Quality Report in CSV or HTML. For example, if you generate a PDF for a Quality Report from a client machine running the English locate and a question in the report is written in Japanese, the data does not appear correctly. The client machine must run in the Japanese locale for the report to display the Japanese text.

Solution. Verify that you are running the correct locale for the supported language on the client machine.

Reporting application does not load

Description. The Reporting application does not load when you click Reporting. The window is blank and a Microsoft Internet Explorer dialog box displays the following message:

```
Errors on this webpage might cause it to work
incorrectly.
Could not load 'dojox.gfx.vml';last tried
../dogox/gfx/vml.js'
```

Solution. Stop the Jetty service, delete the QMDesktop folder from C:\Program Files (x6)\Cisco\WFO_QM\Jetty\work, and then restart the Jetty service.

Error appears when retrieving an evaluation form

Description. When loading a recording from the Recordings application, the following message appears:

```
Error Retrieving Evaluation Form
```

The administrator cleared the Evaluation For Name Check box in Quality Management Administrator. As a result, the evaluation form name does not appear in the Evaluation Form field on the Evaluation pane in the Evaluation and Review application. The recording does not load, and the user cannot playback the recording.

Solution. To resolve this problem, select the Evaluation Form Name check box in Quality Management Administrator.

1. From Quality Management Administrator, choose Recordings > Quality Management > Evaluation Forms > Forms.

   The Evaluation Form Administration window appears.
2. Click the Header tab and then select the Evaluation Form Name check box.
3. Click Save.

Format errors appear in the form and section comments for the Agent Scored Evaluation report

Description. When you generate an Agent Scored Evaluation report, you might see one or more of the following issues.

- Section comments do not wrap.
- Section comments appear to wrap in a saved report, but the first word in the first sentence appears on a line by itself.
- Form comments are truncated.

Solution. Save the report to PDF.

Workforce Optimization and Microsoft Internet Explorer does not support hostnames that contain underscores

Description. The hostname for the Base server must not contain underscores if you are using Microsoft Internet Explorer to access the Workforce Optimization Container.

Solution. Remove underscores in the hostname for the Base server.

Media Player fails to initialize

Description. The Loading pop up for the Media Player appears when you access the Recordings application and hangs.

Solution. Clear the Java cache. To clear the Java cache, perform the following steps:

1. Close your web browser.
2. Choose Start > Control Panel, and then double-click Java.

   The Java Control Panel appears.
3. From the General tab, click Settings.

   The Temporary Files Settings dialog box appears.
4. Click Delete Files, and then click OK.

   The Delete Temporary Files dialog box appears.
5. Click OK to dismiss the dialog box.

   NOTE: It may take several minutes to clear your Java cache.
6. Click OK to dismiss the Temporary Files Settings dialog box.
7. Click OK to dismiss the Java Control Panel.
8. Log into Workforce Optimization, and try again.

Workforce Optimization server is currently offline

Description. A dialog box appears with the following message:

```
We're sorry, but the Workforce Optimization server is
currently offline. When the server returns you will be
automatically redirected to the login page. See your
Workforce Optimization administrator for assistance if
this problem persists.
```

Solution. Verify the services on the Quality Management server are running.

Unable to print report in Adobe PDF or Microsoft Excel

Description: User can successfully print a report to Adobe PDF or Microsoft Excel on the first attempt from Microsoft Internet explorer. When the user tries to print the same report again (two or more times), the report does not print.

Solution: Update the Microsoft Internet Explorer settings. To update the Microsoft Internet Explorer settings, perform the following steps:

> **NOTE:** You need administrative or elevated privileges on your desktop to perform this task.

1. From Microsoft Internet Explorer, choose Tools > Internet Options.

   The Internet Options - Security at Risk dialog box appears.
2. Click the Advanced tab, scroll down to Security, and clear the Do Not Save Encrypted Pages to Disk check box.
3. Click OK to save your changes.

The message, "Stop running this script" appears.

Description: This problem is due to a Microsoft Internet Explorer issue.

Solution: For information on correcting this issue, see Microsoft Support Article ID 175500 available at:

http://support.microsoft.com/kb/175500

The Diagnostics window is blank

Description: When you click Validate my PC Configuration on the Login page, the Diagnostic window is blank.

Solution: If you are running Java 7 Update 25, change the Java security setting from High to Medium.

The Media Player is blank

Description: When you try to access the Media Player, the Media Player is blank.

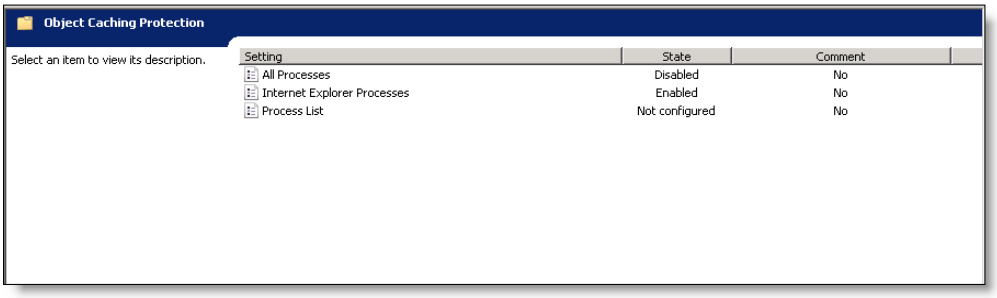
Solution: If you are running Java 7 Update 25, change the Java security setting from High to Medium.

Cisco Unified Workforce Optimization does not load properly in Internet Explorer 9

Description: When you log in to Cisco Unified Workforce Optimization through Internet Explorer 9, the webpage is blank. If you refresh the web browser, the page loads correctly. The expected behavior is that Cisco Unified Workforce Optimization should load properly the first time.

Cause: This problem occurs when a site applies a Group Policy Object (GPO) for PCI compliance to their web browsers through the Group Policy Management Editor. In this instance the group policy security setting, called All Processes under Object Caching Protection, is set to Disabled.

Solution: To keep All Processes set to Disabled and correct this problem, change Internet Explorer Processes to Enabled under Object Caching Protection in the Group Policy Management Editor.



Login page does not appear

Description. When you try to access Workforce Optimization, the Login page does not appear.

Solution. The files in the Jetty work folder are stale. To resolve this issue, perform the following steps:

1. Log in as administrator on the server where the Jetty service is installed.
2. Stop the Jetty service.
3. Delete the contents of the Jetty\work folder. This file is located at C:\Program Files\Calabrio\WFO_QM\Jetty\work.
4. Start the Jetty service.
5. Open a web browser and go to the Workforce Optimization and verify the Login page appears.

Validate my PC configuration does not load with Java 7 Update 55

Description. When you click Validate my PC configuration, the following message appears:

```
The page you are viewing uses Java. More information on Java support
is available from the Microsoft website.
```

When you click OK, the Diagnostic page is blank. You have Java 7 Update 55 or later installed on your client desktop. Java 7 Update 55 is configured for High (minimum recommended) security.

Solution. To resolve this issue, perform the following steps:

1. Enter the following URL in your web browser, where <Base server> is either the IP address or hostname of the user interface.

   `https://<Base server>` or `http://<Base server>`
2. Click Validate my PC configuration.
3. When the following prompt appears, click Run:

   ```
   Do you want to run this application?
   ```
4. When the following prompt appears, click Allow:

   ```
   Allow access to the following application from this web
   site?
   ```

   The Diagnostic window loads successfully.

   NOTE: If the prompts do not appear, it could be that the Java update was recently installed and the machine needs to be restarted. If the prompts do not appear after you reboot the machine, then choose Start > All Programs > Java > Configure Java. From the Java Control panel, click the Security tab and then click Restore Security prompt. Repeat the previous steps after you restore the security prompt.

MANA Issues

CDR Polling failed due to MANA OutOfMemory Error

Description. The following OutOfMemory error appears in the MANA logs.

```
2012-02-07 08:58:28,573 ERROR QMMN2016
[pool-2-thread-1|CmPollingTask#requestProblems:49]
Unexpected error while getting call data for CM
task.2012-02-07 08:58:28,573 STACK QMMN2016
[pool-2-thread-1|CmPollingTask#requestProblems:49]
com.calabrio.qm.mana.cmtask.CallDataException:
Unspecified error comparing CDR and system data. See MANA
log for
details:at com.calabrio.qm.mana.cmtask.CmTask.perform(CmT
ask.java:172)at com.calabrio.qm.mana.tasks.CmPollingTask.
requestProblems(CmPollingTask.java:45)at com.calabrio.man
a.diagnostic.PollingDiagnostic$StatusFuture$1.run(Polling
Diagnostic.java:139)at java.util.concurrent.Executors$Run
nableAdapter.call(Unknown Source)at
java.util.concurrent.FutureTask$Sync.innerRun(Unknown
Source)at java.util.concurrent.FutureTask.run(Unknown
Source)at java.util.concurrent.ThreadPoolExecutor$Worker.
runTask(Unknown
Source)at java.util.concurrent.ThreadPoolExecutor$Worker.
run(Unknown Source)at java.lang.Thread.run(Unknown
Source)Caused by: java.lang.OutOfMemoryError: Java heap
space
```

Solution. Open the manaservice.properties file in the C:\Program Files (x86)\Calabrio\WFO_QM\config folder and change the following line:

```
service4j.jvmOptions=-Dsplk4j.configuration=manaservice.prop
erties | -Xmx256M | -Xrs
```

to:

```
service4j.jvmOptions=-Dsplk4j.configuration=manaservice.prop
erties | -Xmx1024M | -Xrs
```

Service Issues

This topic explains how to diagnose and resolve problems that occur with the services for Quality Management.

Sync service is not synchronizing databases

Description. The Sync service is not synchronizing databases.

Solution. Ensure that the IP address for both Side A and Side B are correct. The IP address and “side” are tied together and are not interchangeable. For example, you cannot specify the IP address for Side B in the Side A field.

Ensure the password is correct for the uccxworkforce login ID.

Verify that you configured the user correctly according to the *Installation Guide*.

Unable to stop the service

Description. When the Quality Management Jetty service restarts or stops, the process gives a warning error message that the system is unable to stop the service.

Solution. In fact, the Quality Management Jetty service really stops at that point. It was shut down before it was fully initialized. The user is able to manually restart the Quality Management Jetty service cleanly.

Troubleshooting a Call Flow by Symptoms

The following table describes at a high level the most important logs to gather for various call flow symptoms. The logs are listed in priority order. It is recommended that you gather all logs from all services.

In general, if your are having problems with the creation of RAW files, the log for the Load-balancing Subscription service is the most important log to gather. Once files are recorded and converted the problems are more likely to be related to upload or workflows, so the logs for the Data API, Upload Controller, and Recording services become more important.

High-level Symptom	Logs to Gather	Possible Cause
No RAW files are being created	1. Load-balancing subscription service 2. Recording service	1. No SIP invite (check the Load-balancing Subscription service log) 2. The device is not configured for a Recording Cluster (check the VoIP Devices window in Quality Management Administrator
RAW or SPX files are stuck on the client machine	1. Recording service 2. Upload Controller service 3. DB Proxy service 4. Data API service	1. The connection to the Upload Controller might be down 2. Database connection or queries might have an issue 3. File might not currently be set for upload or deletion (check the Upload Controller log for the recording ID) 4. File might not currently be reconciled

High-level Symptom	Logs to Gather	Possible Cause
INI files are not being removed (recording files are not being renamed)	1. Example of the INI file **IMPORTANT:** Do not remove the INI file. 2. Recording service 3. Upload Controller service	1. The connection to the Upload Controller might be down 2. Database connection or queries might have an issue 3. File might not currently be set for upload or deletion (check the Upload Controller log for the recording ID)
Workflow problems	1. Data API service 2. Recording service	
Hot Desking problems	1. Data API service 2. Recording Controls (if it is being used) 3. Recording service	
Extension Mobility problems	1. Load-balancing Subscription service 2. Data API service	
General Upload problems	1. Recording service 2. Upload Controller service 3. DB Proxy service 4. Data API service	
General Recording Problems	1. Load-balancing Subscription service 2. Recording service	

Index