



Cisco Unified Workforce Optimization

Quality Management Installation Guide

Version 10.0(1)

First Published: November 30, 2013

Last Modified: July 20, 2016

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Book Title

© 2008-2015 Cisco Systems, Inc. All rights reserved.

© 2008-2015 Calabrio Inc. All rights reserved.

Contents

Overview	15
-----------------	-----------

Quality Management Components 17

- Client Applications 17
 - Quality Management Administrator 17
 - Calabrio Screen Player Plug-in 17
 - Desktop Recording Service 17
 - Calabrio Quality Management Media Player 18
- Web Applications 18
 - Workforce Optimization 18
- Services 18
 - Monitoring and Recording Data API Service 19
 - Monitoring and Recording DB Cleaner Service 19
 - Monitoring and Recording DB Proxy Service 19
 - Monitoring and Recording Jetty Service 19
 - Monitoring and Recording Monitoring and Notification Service 19
 - Monitoring and Recording Monitor Service 20
 - Monitoring and Recording Network Recording Service 20
 - Monitoring and Recording Sync Service 20
 - Monitoring and Recording Upload Controller 20
 - Monitoring and Recording Contact Reconciliation Service 20
 - Contact Reconciliation 20
 - Load-Balancing Subscription Service 22
 - Monitoring and Recording CTI Service 22
 - Monitoring and Recording MediaSense Subscription Service 23
- Mixed Mode Licensing 23
 - SolutionsPlus 23
 - Compliance Recording Application License 24
 - Quality Management Application License 24
 - Advanced Quality Management Application License 24
 - Upgrading Your SolutionsPlus Licenses 24
 - Calabrio Licenses 24

Compliance Recording License	24
Quality Management License	25
Advanced Quality Management License	25
License and Features	25
• System Architecture	26
Single Server Architecture	26

System Requirements 29

• Unified CCX System Environment	29
• Data Storage Environment	29
• Operating System and Hardware Requirements for a Server	30
• Voice Record Server Requirements and Capacity Guidelines	32
Concurrent Users, Configured Users, and Named Users	32
Single Base Server Configuration	33
Disk Storage Sizing Guidelines	33
Determining Hard Disk Space Requirements	34
Recording Storage Requirements	35
Quality Management Storage Calculator	36
• Microsoft SQL Server Requirements	36
Determining Required RAM	37
• Operating Environment	38
Workforce Optimization and/or Quality Management Administrator (No Recording)	38
NIC Requirements	38
QM, QMA, CR, and CRA License (Voice Recording Only)	39
QM, QMA, CR, and CRA License (Voice Recording plus Client Applications)	39
AQM or AQMA License (Voice and Screen Recording)	40
AQM or AQMA License (Voice and Screen Recording plus Client Applications)	41
Quality Management in a Cisco UCS Environment	41
Virtual Server Environment	41
• Required Third-Party Software	42
Server Requirements	42
• Firewall Requirements	43

Jetty Service Ports	43
Changing the Port used by Reporting Services	44
Base Server	44
Recording CTI Server	44
Database Server	45
MediaSense Subscription Server	45
Monitor Server for Server Recording Deployments Only	46
Voice Record Server	46
Site Upload Server	46

Recording Methods 49

• Recording Architectures	49
• Agent Recording	50
Points to remember	50
Desktop Recording (Endpoint) Service Requirements	51
Desktop Recording Considerations	51
Hot Desking	52
Extension Mobility	52
Hard Disk Drive Space on Agent's Computers	52
Network Interface Cards	52
Phone Configurations for the Desktop Recording Service	53
Supported Remote Agent Configurations	54
Hardware VPN Support for Desktop Recording	54
Software VPN support	54
Network Recording	54
Configuring Cisco Unified CM for Live Voice Recording	56
Extension Mobility	57
CTIOS Agent Greeting	58
Supported Remote Agent Configurations	58
Hardware VPN Support for Network Recording	58
Software VPN Support for Network Recording	58
Server Recording (SPAN)	58
Configuring Cisco Unified CM for Live Voice Recording	59
Extension Mobility	60
Supported Remote Agent Configurations	61

Software VPN Support for Server Recording	61
Monitoring Server Considerations	61
• Cisco MediaSense	61
Cisco MediaSense and Cisco Unified CM	62
Cisco MediaSense continues Recording when Quality Management is Offline	62
MediaSense Clusters	63
Redundant Recording with Cisco MediaSense	63
Cisco MediaSense Recording Scalability	63
Cisco MediaSense Cluster and Scalability	64
• Required Codecs	65
Supported Codecs for Unified CCX	65
• Shared Lines	65
• Supported IP Phones	66
Supported Phones for Desktop Recording	66
Supported Phones for Server Recording	67
Supported Phones for Network Recording	67
Supported Phones for MediaSense Recording	67
Cisco IP Communicator Considerations	67
Cisco Jabber	67
Qualifying Phones for Quality Management	68
• Supported Cisco Unified Outbound Dialer Modes	68

Resiliency Options **69**

• High-level Call Flow	69
• CTI and Signaling Services	69
• Load Balancing	69
• Quality Management	70
Application	70
User Licensing	70
Quality Management SQL Database	71
Recording Storage Share for Quality Management	71
User Synchronization Service with ACD	72
Call Event Notification	72
Quality Management CTI Service	72

Recording Services	72
Recording Clusters	73
Distributed Desktop Recording Services	73

Planning Ahead 75

• Pre-installation and Deployment Checklists	75
• Pre-Installation Checklists	75
Pre-Installation Checklist	76
Cisco Unified CM Configuration Checklist	78
Cisco Unified CCX Configuration Checklist	80
• Deployment Checklists	80
Server Installation Checklist	81
Configuration Checklist	82
Application Installation Checklist	83
Optional Configuration Checklist	84
Testing Checklist	85

Before Installing Quality Management 87

• Microsoft Windows Servers	87
Microsoft Windows Server Guidelines	87
Windows Server 2008	87
Enabling Desktop Experience on Windows Server 2008	87
• Microsoft SQL Server	88
All Versions of Microsoft SQL Server	88
Installing Microsoft SQL Server	88
Microsoft SQL Roles	88
Microsoft SQL Server Maintenance Plan	89
Microsoft SQL Server 2008 Standard and Express Editions	90
Microsoft SQL Server 2008 Requirements	90
Adding Firewall Exclusions by Program	90
SQL Server Browser	91
Microsoft SQL Server 2008 Express Edition Considerations	91

- Windows SNMP Services 92
 - SNMP Requirements 92
 - Installing the Windows SNMP Services on Windows Server 2008 92
 - Configuring SNMP 93
 - Add the Public Community 93
 - Configure Security 93
- JTAPI User 94
- Active Directory 94
 - Active Directory Configuration Guidelines 95
 - Active Directory Information 95
 - Locating the Active Directory Domain Name 96
- Citrix or Windows Terminal Services 96
 - Citrix Requirements 97
- External Storage 97
- Cisco Unified CM 98
 - Enabling Required Phone Device Parameters 98
 - Configuring Cisco Unified CM Administration for Network Recording 99
 - Creating a User in Cisco Unified CM 100
- Informix JDBC Driver 101
- Cisco Finesse 101
- Fully Qualified Domain Name 102
- Supporting Asian Languages or Unicode Font 102
 - Installing Supplemental Language or Unicode Font Support 102
 - Supporting Asian Languages or the Unicode Font in PDF Reports 103

Upgrading from Previous Versions 105

- Automated Update Feature 106
- Proxy Host 106
- Mark for Quality Feature 106
- Sites 106
- Telephony Groups 107
- Unified CM Configuration 107
- Extend Screen Recording 108
- Agent Recording 108
- Cluster Recording 108

-
- Recordings Folder 109
 - Configured Devices 109
 - Integration Configuration 109
 - Informix Client Software Development Kit 109
 - Upgrading from Quality Management 8.x(x) to 10.0 110
 - Upgrading the Client Applications 111
 - Testing the Upgrade on Client Desktops 112
 - Verifying the Upgrade is Installed Correctly on the Server 113

Installing Quality Management 115

- Services for Quality Management 115
 - Install Services on a Single Server 116
 - Install Services on Multiple Servers 117

Installing a Service Release or Patch 121

- Guidelines for Installing a Patch (SR, ES, or ET) 122
- Install a Patch (ES or SR) 122
- Rolling Back to a Previous State 123

Running System Configuration Setup 125

- Run System Configuration Setup 126
- Manually Installing the Cisco JTAPI Client 130
- System Configuration Setup Interface 132
 - System Database 132
 - Configuration Settings Used By Services 133
 - Cisco Unified CC Database 134
 - Configuration Settings Used By Services 136
 - Touch-Point Filtering 136
 - Telephony Groups 138
 - Telephony Group Configuration 139

Unified CM Configuration	140	
Unified CM Configuration Settings Used By Services		143
Adding a Backup CTI Service	143	
Subscriber Configuration	145	
Subscriber Configuration Settings Used By Services		146
MediaSense Configuration	147	
MediaSense Configuration Settings Used By Services		148
Enterprise Settings	148	
Configuration Settings Used By Services		150
Sharing Workforce Optimization with Multiple Products		150
Share Login Fields	150	
License	151	
Licensing Rules	151	
Importing a License File	152	
Cleanup	152	
Active Directory	152	
Domain Information	153	
Managing Active Directory Domains		156
SMTP Configuration	156	
Configuring the SMTP Settings for Email		158
SNMP Configuration	158	
Configuring the SNMP Settings		159
CDR Configuration	160	
CDR Information Formats for the QM3002 Notification Trigger		161
Summary Only	161	
Detail (Tab Delimited)	161	
Detail (Plain Text)	162	
Managing Ignored Extensions		162
Allow Emailing of Reports	162	
Session Timeout Options	162	
Locale	163	
Changing the Default Locale		163
Site Settings	164	
Configuration Settings Used By Services		167
Site Considerations	168	
Software Updates	169	
Patches	170	

Managing Site Settings	170
Inclusion List	171
Managing Extension Patterns	173
Monitoring and Notification	174
Configuration Settings Used By Services	177
Configuring the QM3002 Notification Trigger	177
Notification Distribution	178
Managing Notification Distribution Lists	179
Enabling or Disabling a Notification Trigger	180
Examples of Notification Configuration Problems	181
Status	183
Configuration Settings Used By Services	183
• Entering Configuration Data in Update Mode	183
Rules for Upgrading or Modifying the Unified CC Database in Update Mode	183
Stopping the Sync Service Before Upgrading the Unified CCX Database	184
Changing the Base Server	184
Changing Quality Management Configuration Data in Update Mode	186
• System Configuration Setup Tools	186
Start Local Services	188
Create Database Catalogs	188
Generate Info for MSI Clients	188
Download/Install JTAPI	188
Encrypt Audio Files	188
Set Recording Home Directory	188
Show Proxy Network Administrator	188
Generate SSL Certificate	189
Test CTI Services	189
Test MediaSense Subscription Service	189
Display Metadata Encryption Key	189
Choose Monitor Adaptor	190
Remove Recording Services	190
Set Temporary Recording Directory	190
SIP Trunk Certificate	190
Generate SIP Trunk Certificate	190
Upload SIP Trunk Certificate	190

-
- Download SIP Trunk Certificate 191
 - External Storage and Services 191
 - Configuring Services for External Storage 191

Installing Server Applications 193

- Installing the Recording Thin Client on a Citrix Server 193
- Configuring the Audio Player for Citrix 193
 - Configuring the Audio Player Type for Citrix 194

After Installing Quality Management 195

- CAD Integration 195

Installing Client Applications 197

- Enabling the Elevated Privileges Policy for Windows Installer Installation 197
 - Enabling the Windows Elevated Privileges Policy 197
- Using Automated Package Distribution Tools 198
 - Requirements 198
 - Execution 198
 - Per-Machine vs. Per-User 198
 - Automated Package Installation vs. Manual Installation 198
 - Multiple Software Releases 199
 - Recommended Deployment Preparation Model 199
 - Client Installation Packages 199
 - Configuring Client Installation Files 200
- Installing Client Applications for Quality Management 200
 - Enabling the Next Generation Java Plug-in 201
 - Installing Client Applications for Quality Management 201

Removing Quality Management 8.x(x) or later 203

- Removing a Quality Management Application 204
- Removing the Quality Management Databases 205

Backup and Restore 207

- Quality Management Database Disaster Recovery 207
 - Backing Up the Quality Management Databases 207
 - Restoring the Quality Management Database 208
- Genesys Connector Properties File Disaster Recovery 208

Overview

This document explains how to install Cisco Unified Workforce Optimization Quality Management 10.0 in a Cisco Unified Contact Center Express (Unified CCX) environment.

Quality Management Components

The following client applications and services make up the Quality Management system.

Client Applications

You can install the Quality Management client applications from web pages that reside on the Quality Management Base server (Base server). See [“Installing Client Applications” on page 197](#) for instructions on installing the client applications.

Quality Management Administrator

Use Quality Management Administrator to assign user roles, set up groups, create evaluation forms, manage evaluation forms, set up workflows for recording customer contacts, set up recording archiving, and maintain the Quality Management system.

By default, Quality Management installs Quality Management Administrator on the Base server. Using Quality Management Administrator on the Base server ensures that all features under System Configuration are enabled.

You can also install Quality Management Administrator on the client desktop assigned to the Quality Management administrator. When you install Quality Management Administrator on a client desktop, the features under the System Configuration node that allow you to configure information on the Base server are disabled. To modify these features, use either the Quality Management Administrator or System Configuration Setup (PostInstall.exe) on the Base server.

Calabrio Screen Player Plug-in

The Calabrio Screen Player Plug-in plays back screen recordings from the Recordings application.

The Calabrio Screen Player Plug-in must be installed on client desktops that belong to users who will play back screen recordings.

Desktop Recording Service

The Desktop Recording service is responsible for:

- Screen recording and upload for Gateway Recording, Network Recording, and Server Recording
- Voice recording, screen recording, and upload for Desktop Recording (Endpoint)

The Desktop Recording service must be installed on all Endpoint voice recording client desktops and screen recording client desktops.

If a user is configured for Network Recording or Server Recording and the agent's desktop is daisy-chained to a phone, voice recording occurs on the server.

Calabrio Quality Management Media Player

The Calabrio Quality Management Media Player (Media Player) is responsible for recording playback control.

The Media Player is installed on the client desktop when the user first accesses the Recordings application.

Web Applications

You access the Quality Management web applications from a web browser.

Workforce Optimization

Use Workforce Optimization to perform the following tasks:

- View the contact center's performance statistics for the last twelve months by agent, team, and group
- Search stored archives for specific contact
- Evaluate contact for quality management
- Monitor active calls
- Monitor the recording status of active calls
- Generate evaluation reports and system reports

Services

You can install services from the Quality Management setup executable. See ["System Architecture" on page 26](#) for information on where these services reside.

Monitoring and Recording Data API Service

The Monitoring and Recording Data API (Data API) service is the interface between the Jetty webserver and the database.

The Data API service evaluates a quality workflow based on current End of Day (EOD) time. If the EOD time changes, the Data API service is notified immediately and all calls will be processed using the new EOD time.

The Data API service will process quality workflow in 24-hour batches based on current EOD. (At most, it will process 10 days worth of unprocessed contacts per session.)

Monitoring and Recording DB Cleaner Service

The Monitoring and Recording DB Cleaner (DB Cleaner) service purges the following data on a daily basis:

- Records from the Quality Management database
- Media files from the Site Upload server

Monitoring and Recording DB Proxy Service

In Monitoring and Recording Services deployments, the Monitoring and Recording DB Proxy (DB Proxy) service is the point of connection between the Upload Controller and the Quality Management database.

The DB Proxy service tells the Upload Controller when to upload or delete a recording. If not enough information is known about a recording to indicate that it should be updated or deleted, the DB Proxy service tells the Upload Controller to ask again at EOD.

Monitoring and Recording Jetty Service

The Monitoring and Recording Jetty (Jetty) service webserver hosts the Quality Management Reports webapp, C1Surrogate webapp, File Transfer Servlet (FTS), Server API engine, and Licensing webapp.

Monitoring and Recording Monitoring and Notification Service

The Monitoring and Recording Monitoring and Notification (MANA) service polls the Quality Management system for problems. When there are problems, the MANA service sends alerts to the administrators through the event viewer, email, or SNMP. You can select the problems that trigger the notification in Quality Management Administrator.

Monitoring and Recording Monitor Service

The Monitoring and Recording Monitor (Monitor) service works in conjunction with the Network Recording service for Server Recording. The Monitor service filters the packets coming from a Switched Port Analyzer (SPAN) session and forwards the packets to the Network Recording service for recording.

Monitoring and Recording Network Recording Service

The Monitoring and Recording Network Recording (Network Recording) service records voice for agents who are configured for Server Recording, Network Recording, or Gateway Recording.

Monitoring and Recording Sync Service

The Monitoring and Recording Sync (Sync) service synchronizes the agents and supervisors, every 10 minutes from Unified CCX.

Monitoring and Recording Upload Controller

The Monitoring and Recording Upload Controller (Upload Controller) service manages the upload of recordings and call metadata from the recording clients.

Monitoring and Recording Contact Reconciliation Service

The Monitoring and Recording Contact Reconciliation (Contact Reconciliation) service gathers all information for a call recording received through the Session Border Controller (SBC) and stores the contact information for the call in the Quality Management database,

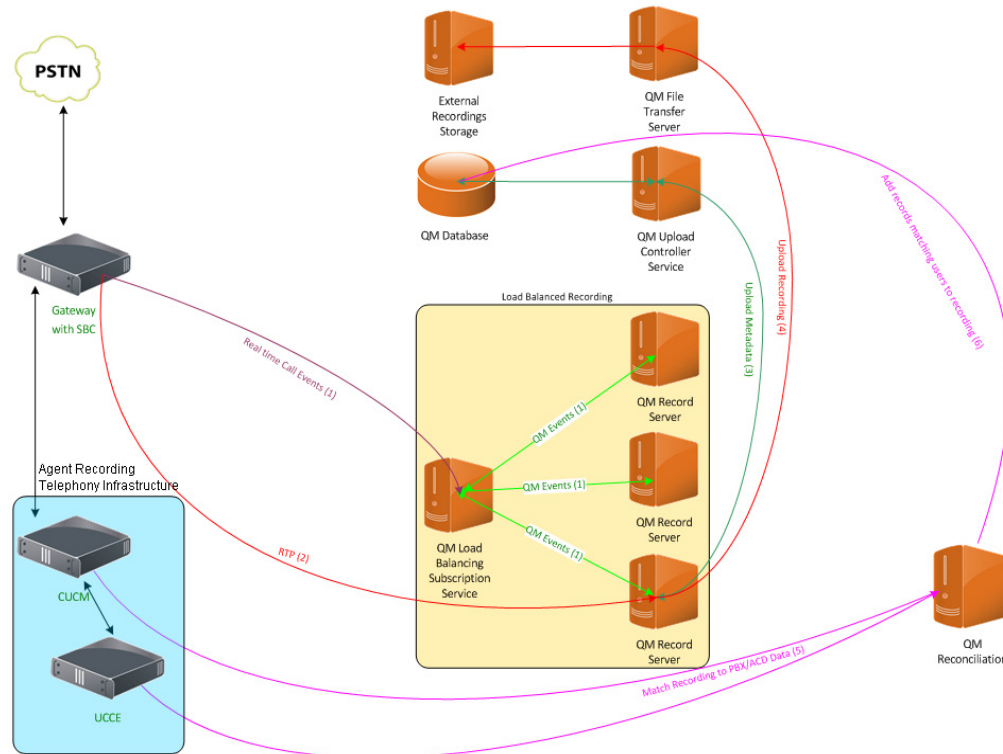
Contact Reconciliation

Contact reconciliation is the process of gathering call-related data from one or more external sources and cross-referencing it with the sparse data (for example, ANI, DNIS, extension, or some type of gateway call identifier) that the call provided with the call recording. When a call recording is reconciled, the contact record is stored in the Quality Management database. Remember that a call recording might involve several agents. The time a specific agent was on a call is included in the database. You can use the search feature in the Recordings application to search for the agent associated with a specific call recording and then play back or evaluate the portion of the call recording that is associated with that agent.

Contact reconciliation occurs after the call data has been uploaded and before the recording is uploaded to permanent storage (see [Figure 1](#)). Reconciliation will use the

call data that was uploaded to the system database to determine which users, if any, participated in the call recording.

Figure 1. Contact reconciliation

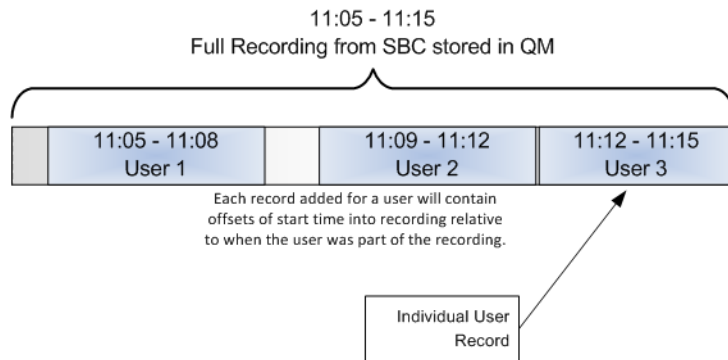


Each call recording will contain a unique ID that originated at the SBC. The contact reconciliation process uses that unique ID to determine which users participated in the call during the time it was recorded. The contact reconciliation process will then update the system database with the new user information and any metadata associated with the call based on information gathered from the PBX/ACD.

After the contact reconciliation process has run, the original call will be available for playback, but not for quality management or quality scoring. Additional records for that call will be available that include the person(s) associated with the call and when the time they were on the call.

For example, if a call recording runs from 11:05 to 11:15, that call will be available for playback right after the recording ends. If User 1 is on the call from 11:05 to 11:08, User 2 from 11:09 to 11:12 and User 3 from 11:12 to 11:15, there will be four records available for playback after reconciliation has run. The records include the original call and records for users 1, 2, and 3 (see [Figure 2](#)). The records for users 1, 2, and 3 contain the data for when those users were on the call and will be available for quality scoring.

Figure 2. Contact reconciliation example



Load-Balancing Subscription Service

Quality Management provides the following load-balancing subscription services:

- [Monitoring and Recording CTI Service](#)
- [Monitoring and Recording MediaSense Subscription Service](#)

Use the load-balancing subscription service that is best suited for your environment.

When a call event goes through the SBC, the load-balancing subscription service receives an event with information related to the call and sends it to the Network Recording service that is associated with a Voice Record Server in a Recording Cluster. The load-balancing subscription service also performs load balancing on call events to the Voice Record Servers that are registered with the load-balancing subscription.

The Voice Record Server either records the Real-time Transport Protocol (RTP) or retrieves the call recording made by another recording system (for example, MediaSense). The Network Recording service downloads the raw data files, stores them in the Recordings folder, and writes the data associated with the call to the database.

You can also use the load-balancing subscription service to improve resiliency.

Monitoring and Recording CTI Service

The Monitoring and Recording Computer Telephony Integration (CTI) service (Recording CTI service) creates a monitoring session using the Cisco Unified Communications Manager (Unified CM) Java Telephony Application Programmer Interface (JTAPI) client to get call control events and status updates from monitored devices.

The Recording CTI service sends events to the Network Recording service when there is a change in the status of monitored phones. The recording CTI service also sends screen recording start/stop signals to the recording clients.

Install this service if you plan to use Desktop Recording, Network Recording, or Server Recording (SPAN).

Monitoring and Recording MediaSense Subscription Service

The Monitoring and Recording MediaSense Subscription (MediaSense Subscription) service registers Cisco MediaSense events. When a call is recorded on the Cisco MediaSense cluster for a registered device, this service receives an event with information related to the call recording and sends it to the Network Recording service that is associated with the VoIP device that was recorded. The Network Recording service downloads the raw data files, stores them in the Recordings folder, and writes the data associated with the call to the database.

Install this service if you plan to use Cisco MediaSense Recording.

Mixed Mode Licensing

You need to assign licenses to the following users:

- Agents and knowledge workers you need to record
- Users who need to access the web applications

You can assign the same license to all users or you can assign a mixture of licenses to users.

The license type determines what Quality Management records. For example, if agents X and Y have an Advanced Quality Management (AQM) license, the application can record their screens.

SolutionsPlus

SolutionsPlus is a set of licenses that support the MediaSense capture method for recordings.

SolutionsPlus only uses the MediaSense Subscription service and does not use the Monitor service. If a user licensed for SolutionsPlus is configured for a different recording capture method, the Recording Cluster will ignore the configuration and the user will not be recorded.

Compliance Recording Application License

The Compliance Recording Application (CRA) license allows only audio recording and archive search and playback. Status and archive reports are available to supervisors and managers only.

Quality Management Application License

The Quality Management Application (QMA) license supports audio contact recordings only for archival and quality management purposes.

Advanced Quality Management Application License

The Advanced Quality Management Application (AQMA) license supports both audio and screen recordings, as follows:

- Audio-only recording for archival purposes
- Screen and audio recordings for quality management purposes

Upgrading Your SolutionsPlus Licenses

If you need more recording capture methods, you can purchase Calabrio licenses. A Calabrio license includes the following recording capture methods:

- Desktop Recording
- Server Recording
- Network Recording
- MediaSense Recording

To add more recording capture methods, you need to:

- Purchase a Calabrio (CR, QM, or AQM) license
- Add more servers, as required, to meet capacity and configuration requirements
- Install the appropriate Load-balancing Subscription service and the Monitor service, if they were not previously installed
- Switch users to the Calabrio license

Calabrio Licenses

Calabrio provides a set of licenses that use the Calabrio capture method for recordings.

Compliance Recording License

The Compliance Recording (CR) license allows only audio recording and archive search and playback. Status and archive reports are available to supervisors and managers only.

Quality Management License

The Quality Management (QM) license supports audio contact recordings only for archival and quality management purposes.

Advanced Quality Management License

The Advanced Quality Management (AQM) license supports both audio and screen recordings, as follows:

- Audio-only recording for archival purposes
- Screen and audio recordings for quality management purposes

License and Features

[Table 1](#) shows the Quality Management features available by license for Cisco Unified CCX.

Table 1. License and features for Cisco Unified CCX

Feature	Calabrio Licenses			SolutionsPlus Licenses		
	CR	QM	AQM	CRA	QMA	AQMA
100% voice recording and archiving	x	x	x	x	x	x
Live voice monitoring	x	x	x	x	x	x
Desktop Recording, and Network Recording	x	x	x	--	--	--
Cisco MediaSense Recording	x	x	x	x	x	x
Search utility	x	x	x	x	x	x
On-demand recording	x	x	x	x	x	x
Recording with or without a PC	x	x	x	x	x	x
Monitoring and Notification (MANA) administration	x	x	x	x	x	x
Quality evaluations	--	x	x	--	x	x
Screen recording	--	--	x	--	--	x

System Architecture

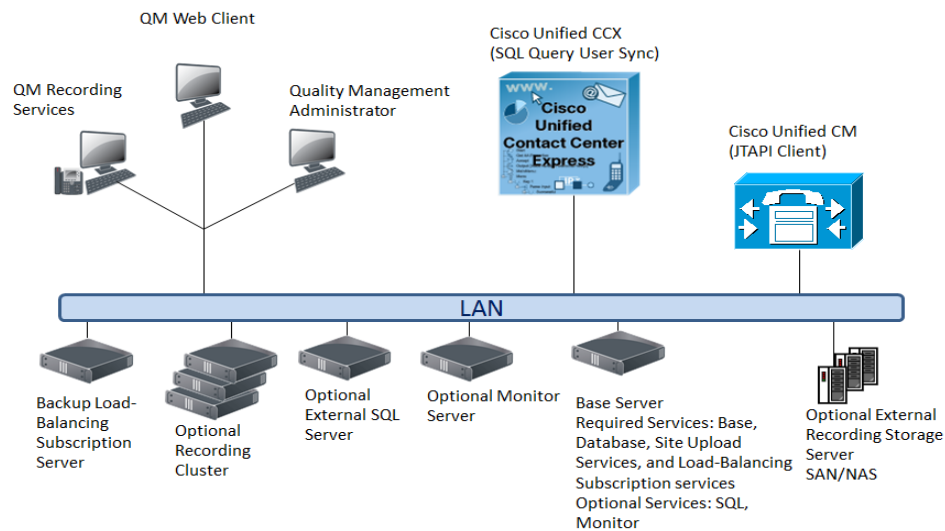
For a Cisco environment running Unified CCX: Quality Management supports one system architecture. This architecture is able to use an optional external storage server to store voice and screen recording files.

Additionally, Quality Management requires one dedicated CTI server for each Unified CM cluster. For example, if there are two Unified CM clusters, then there must be two CTI servers.

Single Server Architecture

Figure 3 show an example of a single server architecture.

Figure 3. Single server architecture



Single server architecture consists of the Base server and can include the following optional servers:

- Backup Load-Balancing Subscription server—including one of the following Load-Balancing Subscription services:
 - CTI service—for Desktop Recording, Network Recording, or Server Recording. One CTI service per Cisco Unified CM cluster in a Cisco environment is required.
 - MediaSense Subscription Service
- Voice Record Server—on-board or off-board
- Optional Recording Cluster

- Monitor server—on-board or off-board
- Record and Monitor server—on-board or off-board
- Optional external recording storage server
- Optional external server hosting Structured Query Language (SQL) server

Table 2 shows how the services are bundled and where they are used in single server architecture.

Table 2. Bundled services for Quality Management

Server	Services Bundle	Services
Base server	Base Services	<ul style="list-style-type: none"> • Monitoring and Recording Data API Service • Monitoring and Recording Jetty Service • Monitoring and Recording Monitoring and Notification Service • Monitoring and Recording Sync Service
	Database Services	<ul style="list-style-type: none"> • Monitoring and Recording DB Cleaner Service • Monitoring and Recording DB Proxy Service
	Site Upload Server	<ul style="list-style-type: none"> • Monitoring and Recording Jetty Service • Monitoring and Recording Upload Controller • Screen Playback Gateway Service
	Choose one of the following services: <ul style="list-style-type: none"> • CTI Services 	<ul style="list-style-type: none"> • Monitoring and Recording CTI Service—for Desktop Recording, Network Recording, or Server Recording • Monitoring and Recording MediaSense Subscription Service—for Cisco MediaSense Recording
Base server or Voice Record Server (Optional)	Recording Services (optional)	Monitoring and Recording Network Recording Service—for Cisco MediaSense Recording, Network Recording, or Server Recording
Base server or Monitor server (Optional)	Monitoring Services (Optional)	Monitoring and Recording Monitor Service—for Server Recording only

Table 2. Bundled services for Quality Management (Continued)

Server	Services Bundle	Services
Gateway Recording server	Reconciliation Services	<p>These services enhance the metadata, and adds the agent name and endpoint extension.</p> <ul style="list-style-type: none"> • Monitoring and Recording Contact Reconciliation—for Cisco MediaSense Recording <p>NOTE: Reconciliation Services are only required for Gateway Recording.</p>
Backup Load-Balancing Subscription server	<p>Choose one of the following services:</p> <ul style="list-style-type: none"> • CTI Services • MediaSense Subscription Service 	<ul style="list-style-type: none"> • Monitoring and Recording CTI Service—for Desktop Recording, Network Recording, or Server Recording • Monitoring and Recording MediaSense Subscription Service—for Cisco MediaSense Recording

NOTE: The Monitor and Network Recording services are optional services. You can choose to install these services on the Base server or separate servers. Cisco recommends installing these services even if you are not using them so you do not have to install them later to use these features.

System Requirements

This topic lists the Quality Management requirements. Read this information carefully and ensure your system environment meets all requirements before you install Quality Management.

Desktop hardware and software requirements are provided in the *Desktop Requirements Guide*.

Unified CCX System Environment

Quality Management supports the following Cisco Unified CCX versions:

- 10.0
- 9.0

See the *Cisco Unified Contact Center Express Compatibility Information* for a complete list of supported combinations. This document is available on the Cisco website (www.cisco.com).

Data Storage Environment

Use one of the following products to maintain and store the system configuration data.

- Microsoft SQL Server 2008 Standard Edition—1 to 4 processors
- Microsoft SQL Server 2008 R2 SP1 Express Edition—See “[Microsoft SQL Server 2008 Express Edition Considerations](#)” on page 91 for more information on requirements.

Standard Edition can support up to four processors. You will need Enterprise Edition if you want to support more than 4 processors.

The Microsoft SQL Server can be coresident on the Base server or database server for up to 500 named users.

Operating System and Hardware Requirements for a Server

[Table 3](#) displays the minimum operating system and hardware requirements for all Quality Management servers. The requirements are based on the server size (for example, small, medium, large, or ultra server).

When determining the size of a server, observe the following guidelines:

- The following servers require the medium server hardware requirements:
 - CTI (subscription) server or backup CTI server
 - Monitor server
 - Site Upload (site storage) server
 - Reconciliation services
- To determine the server hardware requirements for the following servers, determine the server size based on capacity and then use [Table 3](#) to determine the requirements for that server.
 - For the Voice Record Server, see [“Voice Record Server Requirements and Capacity Guidelines” on page 32](#) to determine the server size
 - For a single Base server configuration, see [“Single Base Server Configuration” on page 33](#) to determine the server size
 - For the Microsoft SQL server, see [“Microsoft SQL Server Requirements” on page 36](#) to determine the server size

The Quality Management server scalability is dependent on the number of processing threads.

NOTE: The number of processor cores in your system can be determined by viewing the Performance tab in Windows Task Manager—there is one CPU History Usage graph for every processor core. Note that some types of processors are hyperthreaded, meaning that each physical core is presented as two processor cores. This results in twice the number of processor cores displayed in Windows Task Manager.

Table 3. Server requirements

Operating System	Specifications	Ultra Server	Large Server	Medium Server	Small Server
Windows 2008 Server R2 or later ^a , 64-bit	Processor Cores (Intel)	12	4	2	1
	Processor Cores (AMD)	24	8	4	2
	Processor Cores (VMware)	24	8	4	2
	Minimum Processor Speed ^{b,c}	2 GHz	2 GHz	2 GHz	2 GHz
	Memory (GB)	16	8	4	4
	Minimum IOPS	429	143	143	143
	System Storage (GB) for Operating System and Quality Management	40	40	40	40

- a. Apply Microsoft Windows Server updates as recommended by Microsoft. Quality Management does not have Microsoft dependencies.
- b. The minimum processor recommendations for Intel are Xeon Processor E3 family or higher running above 2 GHz or Xeon Processor 5502 on up. You must enable hyper threading for Intel processors.
- c. The minimum processor recommendation for AMD is Opteron Processor 3000 or higher.

If you are using a Terminal Services or Citrix XenApp for recording purposes, these servers require additional server resources for recording screen. The resource requirements will vary depending on the actual design and might require some detailed hardware designs that should be reviewed by Cisco prior to deployment.

NOTE: If you are planning to use a virtual or Citrix environment, see [“Virtual Server Environment” on page 41](#) or [“Citrix or Windows Terminal Services” on page 96](#) for additional information.

Voice Record Server Requirements and Capacity Guidelines

Use the capacity guidelines in [Table 4](#) to determine the Voice Record Server capacity requirements for a single server configuration.

Table 4. Voice Record Server capacity guidelines

Specifications	Ultra Server	Large Server	Medium Server	Small Server
Audio Media File Storage (GB) ^a	500 ^b	125 ^b	100 ^b	100 ^b
Concurrent Users	1000	300	125	50
Minimum IOPS	429	143	143	143

- a. The temporary recording location on a Voice Record Server (that is, the recordings folder) must be located on disk other than the Operating System disk where Quality Management is installed. Write caching on the disk where recordings are stored must be enabled.
- b. Recording storage varies by use.

Capacity is also affected by the type of recording you choose to implement.

NOTE: To maximize system performance and increase data storage capacity, do not install other applications on the server that host the services for Quality Management.

Concurrent Users, Configured Users, and Named Users

The users are defined as follows:

- Concurrent users—the maximum number of users that will be logged into the system at the same time, or concurrently.
- Configured or Named users—all users of the application who have been configured and licensed within the administrative tool. Cisco WFO application software licensing is based on the number of “named” users. The term configured is sometimes used in place of named when referring to application users and the terms are considered synonymous.

Single Base Server Configuration

The following table displays the capacity guidelines for a single Base server configuration where MediaSense Recording, Server Recording, or Network Recording are co-resident with (or hosted on the same server as) the Quality Management Base Services.

Table 5. Single Base server configuration

	Server Type			
	Ultra Server	Large Server	Medium Server	Small Server
Maximum number of named users for voice and screen recording	5000	2000	1000	500
Maximum number of concurrent agent recordings through subscription service	1500	500	250	125
Maximum number of concurrent agents for MediaSense Recording, Server Recording, or Network Recording are (always voice, no screen option)	500	150	60	25

See [“Recording Storage Requirements” on page 35](#) for additional information on storage requirements and external database requirements.

Disk Storage Sizing Guidelines

To calculate the storage that a contact center will need, you need to collect the following data:

- Number of agents who will be recorded
- Average length of calls that are recorded
- Number of calls that are recorded per agent per day
- Number of work days per agent per month
- Number of months that recordings will be kept

The number of minutes that will be recorded every day is the product of three numbers: the number of agents being recorded, the average call length, and the average number of calls that are recorded for each agent per day.

To estimate the amount of disk storage required for your system, use the following formulas:

Amount	Formula
Daily recorded minutes	Agents × Length × Calls = Recorded
Total recorded minutes to store	Recorded × Days × Months = Stored
Voice recording storage (MB)	Stored × 0.12 MB/minute = Voice
Screen recording storage ^a (MB)	Stored × 1.20 MB/minute = Screen

a. Note that the storage requirements for screen recordings depend on three factors: screen activity, monitor resolution, and the number of monitors being recorded. The value shown here is based on low to moderate screen activity, 768 x 1024 resolution, and a single monitor. This rate may increase by 200-400% when recording dynamic, graphical, or media-intensive applications.

Keep in mind that the criteria that determine which contacts are recorded and how long recordings are kept depends on the purpose of the recording. If you are recording for compliance purposes, only the audio portion of a contact is recorded, and the recording might be retained for as long as 7 years. If you are recording for quality management purposes, contact centers can choose to record either audio only or both audio and video. In either case, only some of the contacts will be recorded, and recordings will be kept for much shorter periods of time, such as 30 or 60 days.

Voice and screen recordings can occupy a great deal of hard disk drive space on the server that hosts the recording file storage location.

To protect the recording file storage location from running out of the free space required for normal operations and to prevent crashes, Quality Management:

- Sends warning alerts through MANA when free disk space falls below 10 GB.
- Halts recording when the available hard drive disk space fall below 2 GB. The recordings remain on the client desktop until you free up disk space on the storage location.

All recording client (endpoint and server) provide a report when disk threshold is below minimum and causes recording to stop. The Voice Record Server will additionally provide full disk space information and recording capacity in the response to the MANA status request.

Determining Hard Disk Space Requirements

All recordings are converted from raw files to SPX when the call ends and then stored in the Recordings folder. They are then uploaded to the recording storage location at End of Day (EOD).

You need to determine your hard disk space requirements for the Voice Record Server. The formula used to determine hard disk space requirements, in GB, for a single server configuration is as follows:

$$A + B + (C \times D)$$

where:

A = Service installations and logs (The value is 40 GB.)

B = Database (The value is 10 GB.)

C = GB (The value is .5 GB for voice recording only or 1 GB for voice and screen recording.)

D = Number of agents

NOTE: Values C and D are only required if you are using an on-board Voice Record Server.

For example:

$$40 + 10 + (.5 \times 100) = 100 \text{ GB}$$

The formula used to determine hard disk space requirements for each off-board Voice Record Server configuration is as follows:

$$A + (C \times D)$$

For example:

$$40 + (.5 \times 300) = 190 \text{ GB}$$

Recording Storage Requirements

The recording storage requirements are as follows:

- Voice only—.5 GB/recorded user
- Voice and screen—1 GB/recorded user

The recording storage requirements specify the amount of disk space required per recorded user for caching the recordings prior to their eventual upload to the Quality Management server. The recordings are stored on the same disk drive where the services are installed.

Quality Management Storage Calculator

The *Quality Management Storage Calculator Storage Server Sizing Spreadsheet* provides a storage calculator you can use to determine your storage requirements. This spreadsheet is available on the Calabrio Portal at:

<http://portal.calabrio.com>

Microsoft SQL Server Requirements

The contact metadata for Quality Management is stored in the Microsoft SQL database on the Microsoft SQL Server. Contact metadata remains in the Microsoft SQL database for the longest of the configured retention periods for the media files or 13 months if the retention period for the media files is less than 13 months. The formula used to estimate the maximum number of contacts stored in the database is as follows:

$$A \times B \times C \times D = E$$

where:

A = Number of Agents

B = Average Number of Recorded Contacts per Day per Agent

C = Number of Days per Month the Contact Center Handles Calls

D = Configured Retention Time in Months

E = Total Saved Contacts in the database

For example:

$$300 \times 25 \times 22 \times 13 = 2.1 \text{ Million Recorded Calls}$$

This example requires an off-board Microsoft SQL Server with a minimum of 4 CPU cores, 6 GB RAM, and Microsoft SQL Server with 64-bit to meet Microsoft SQL Server memory requirements.

To ensure satisfactory response rates from the Microsoft SQL database the resources listed in [Table 6](#) must be available and configured for use by Microsoft SQL on its hosting server. For deployments where Microsoft SQL is coresident with the Base services (for example, the Single Server Architecture or Cisco Unified Computing System (UCS) environment), you can dedicate a maximum of 1 CPU Core and 2 GB RAM to Microsoft SQL from the server resources as listed in [“Voice Record Server Requirements and Capacity Guidelines” on page 32](#) for physical server hardware requirements.

Table 6 uses a core with two processing threads. Intel CPU cores support two processing threads per core and AMD processors perform best with a single processing thread per core. The Quality Management server scalability is dependent on the number of processing threads, so the number of recommended cores for AMD are doubled when compared to Intel.

Table 6. Microsoft SQL Server requirements

Specifications	Ultra	Large	Medium	Small
Total Saved Contacts	12+ million	4-12 million	500K-4 million	< 500K
Microsoft SQL Server Edition	Enterprise	Enterprise	Standard	Express
Width	64 bit	64 bit	64 bit	64 bit
Dedicated Memory for Microsoft SQL Server	12 GB RAM ^a	8 GB RAM	6 GB RAM	2 GB RAM
Requires an Off-board Microsoft SQL Server	Yes	Yes	Yes	No

a. See [“Determining Required RAM” on page 37](#) if the number of saved contacts exceed 12 million.

NOTE: Microsoft SQL Server caches pages so as the available RAM increases, the frequency required by Microsoft SQL Server to access the disk decreases and performance will improve. For large deployments, it is recommended that you monitor usage and performance along with the Performance Monitor (PerfMon) to appropriately size your Microsoft SQL server over time.

Apply Microsoft SQL Server updates as recommended by Microsoft. Quality Management does not have Microsoft dependencies.

Determining Required RAM

If your saved contacts exceed 12 million, use the following formula to determine the required RAM:

$$A \div 2 = B$$

where:

A = Number of Million Contacts Saved

B = Number of Gigabytes RAM

For example:

$$110 \div 2 = 55 \text{ GB RAM}$$

This example assumes you have 110 million Contacts Saved and requires an off-board Microsoft SQL Server with a minimum of 16 CPU cores and Microsoft SQL Server with 64-bit to meet Microsoft SQL Server memory requirements.

Operating Environment

Quality Management runs in the operating environment described in the following topics.

Workforce Optimization and/or Quality Management Administrator (No Recording)

Table 7 displays the minimum hardware requirements for Workforce Optimization and/or Quality Management Administrator without recording.

Table 7. Workforce Optimization and/or Quality Management Administrator (no recording)

Operating System	Minimum Hardware Requirements
Windows XP Professional, including the latest Service Pack	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/314865 .
Windows Vista Business, Enterprise, and Ultimate Editions, 32 or 64-bit, including the latest Service Pack	100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/919183 .
Windows 7 Professional and Ultimate, 32 or 64-bit	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-US/windows7/products/system-requirements .

NIC Requirements

NICs must support Promiscuous Mode. See the *Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring*

documents for more information on the Promiscuous Mode and testing a NIC's capabilities. These documents are available on the Cisco website (www.cisco.com).

QM, QMA, CR, and CRA License (Voice Recording Only)

Table 8 displays the minimum hardware requirements for QM, QMA, CR, and CRA license for voice recording only.

Table 8. QM, QMA, CR, and CRA license (voice recording only)

Operating System	Minimum Hardware Requirements
Windows XP Professional, including the latest Service Pack	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/314865 .
Windows Vista Business, Enterprise, and Ultimate Editions, 32 or 64-bit, including the latest Service Pack	100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-us/windows-vista/products/system-requirements .
Windows 7 Professional and Ultimate, 32 or 64-bit	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-US/windows7/products/system-requirements .

QM, QMA, CR, and CRA License (Voice Recording plus Client Applications)

Table 9 displays the minimum hardware requirements for QM, QMA, CR, and CRA license with voice recording plus client applications.

Table 9. QM, QMA, CR, and CRA license (voice recording plus client applications)

Operating System	Minimum Hardware Requirements
Windows XP Professional, including the latest Service Pack	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/314865 .

Table 9. QM, QMA, CR, and CRA license (voice recording plus client applications)

Operating System	Minimum Hardware Requirements
Windows Vista Business, Enterprise, and Ultimate Editions, 32 or 64-bit, including the latest Service Pack	100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-us/windows-vista/products/system-requirements .
Windows 7 Professional and Ultimate, 32 or 64-bit	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-US/windows7/products/system-requirements .

AQM or AQMA License (Voice and Screen Recording)

Table 10 displays the minimum hardware requirements for AQM or AQMA license using voice and screen recording.

Table 10. AQM or AQMA license (voice and screen recording)

Operating System	Minimum Hardware Requirements
Windows XP Professional, including the latest Service Pack	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/314865 .
Windows Vista Business, Enterprise, and Ultimate Editions, 32 or 64-bit, including the latest Service Pack	2 GHz processor 2 GB of system memory 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-us/windows-vista/products/system-requirements .
Windows 7 Professional and Ultimate, 32 or 64-bit	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-US/windows7/products/system-requirements .

AQM or AQMA License (Voice and Screen Recording plus Client Applications)

Table 11 displays the minimum hardware requirements for AQM or AQMA License using voice and screen recording plus client applications like Workforce Optimization and/or Quality Management Administrator.

Table 11. AQM or AQMA License (voice and screen recording plus client applications)

Operating System	Minimum Hardware Requirements
Windows XP Professional, including the latest Service Pack	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://support.microsoft.com/kb/314865 .
Windows Vista Business, Enterprise, and Ultimate Editions, 32 or 64-bit, including the latest Service Pack	2 GHz processor 2 GB of system memory 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-us/windows-vista/products/system-requirements .
Windows 7 Professional and Ultimate, 32 or 64-bit	2 GB RAM 100 Mbit NIC For additional hardware requirements, see http://windows.microsoft.com/en-US/windows7/products/system-requirements .

Quality Management in a Cisco UCS Environment

Quality Management is certified to run on any Cisco Unified Computing System (UCS) server with resources available to support the OVA/OVF template.

The virtual server requirements for deployments on UCS servers are specified on the Cisco wiki page “Virtualization for Cisco Unified Work Force Optimization Suite for Cisco Unified Contact Center Express” located at this URL:

http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unified_Work_Force_Optimization_Suite_for_Cisco_Unified_Contact_Center_Express

Virtual Server Environment

A virtual server environment requires hardware resources equivalent to those required for a physical server (see [“Operating System and Hardware Requirements for a Server” on page 30](#)).

The supported versions of VMware ESX or ESXi virtual servers are the following:

- VMware ESX 3.0
- VMware ESX 3.5
- VMware ESXi 4.0
- VMware ESXi 4.1
- VMware ESXi 5.x

IMPORTANT: VMware Snapshots is only supported for Quality Management when calls are not being recorded. A snapshot impacts server resources that are critical to Quality Management. Recording failures will occur if snapshots are taken while Quality Management is recording calls. Before you take a snapshot, verify that there is no current recording activity and stop the services for Quality Management or pause or shut down the server. You can use the Recording Monitoring application to verify that there are no calls currently being recorded. After you take a snapshot you must restart Quality Management services. You can restart services for Quality Management by restarting the appropriate Load-balancing Subscription service or running a service restart script.

It is recommended that you use the following settings to reduce the possibility of performance issues when running Quality Management on virtual machines:

- Shares—guarantee that VMs are given a percentage of an available resource (CPU, RAM, Storage I/O, Network)
- Limits—guarantee that a VM does not consume more than a specified resource limit
- Resource Reservation—provides an allocated resource for a VM on startup

If you are using VM in a VMware environment, install the Quality Management application in its own computing environment that is not shared with? multiple hosts.

Required Third-Party Software

Quality Management requires the following third-party software in order to run successfully. These applications are not installed when you install Quality Management. They must be purchased and installed separately.

Server Requirements

Quality Management one of the following Microsoft SQL Servers installed on the Base server or an offboard server.

- Microsoft SQL Server 2008 64-bit Standard Edition Service Pack 2
- Microsoft SQL Server 2008 R2 SP1 Express Edition¹

Informix Client SDK for Windows x86_64, 64-bit, version 3.70FC7DE, is required on the Base server for the database.

Firewall Requirements

For Quality Management to function correctly, the ports listed in this section must be opened in the Windows Firewall. If the Windows Firewall/Internet Connection Sharing (ICS) service is running when Quality Management is installed, the Quality Management installation process opens all ports and programs as needed except those for:

- Microsoft SQL Server (by default, 1433 and 1434)
- Informix Client SDK (by default, 1504)

See [“Microsoft SQL Server” on page 88](#) for information on adding Windows Firewall exclusions and allowing remote connections for Microsoft SQL Server and Informix Client SDK.

If another firewall is used, or if you start the Windows Firewall/ICS service and then turn on the Windows Firewall after Quality Management is installed, the ports must be opened manually. See your firewall documentation for instructions.

NOTE: Any non-Cisco services that use the ports listed in this section must be configured to use a different port.

Jetty Service Ports

The Monitoring and Recording Jetty service uses TCP ports 80 and 443. Make sure that you do not have any other web service that use these ports installed on the Base server and Site Upload server or the Jetty service might fail. Examples include Microsoft SQL Server 2008 Reporting Services and Microsoft Internet Information Services (IIS).

1. This option is for smaller customer sites that expect to stay within the 10 million contact limit. See [“Microsoft SQL Server 2008 Express Edition Considerations” on page 91](#) for more information on requirements.

SQL Server 2008 Reporting Services is a tool that provides a web-based GUI to present SQL performance information. You can configure this tool to use another port so it does not interfere with the Jetty service.

Changing the Port used by Reporting Services

TASK

1. On the server hosting SQL Server 2008, launch Reporting Services Configuration Manager (Start > Microsoft SQL Server 2008 > Configuration Tools > Reporting Services Configuration Manager).
2. Connect to the report server instance.
3. In the left pane, click Web Service URL. In the right pane, under Report Server Web Service Site Identification, change the TCP port from 80 to another port (for example, 8080).
4. In the left pane, click Report Manger URL. In the right pane, click Advanced and in the resulting window change the TCP port from 80 to another port (for example, 8080).
5. Click Apply, and then exit the Configuration Manager.

Base Server

Table 12 lists the ports on the Base server that must be opened in the Windows Firewall.

Table 12. Port usage for the Base server

Port/Program	Type	Service
80	TCP	Jetty service (Jetty port)
443	TCP	Jetty service (Jetty SSL port)
8088	TCP	Jetty service (Automated Update)
59011	TCP	Sync service
59103	TCP	Jetty service (Data API service) ^a

a. The surrogate port is located on the Base server. The Data API Service uses this port to communicate with the Surrogate through the Jetty service.

Recording CTI Server

Table 13 lists the ports on the recording CTI server that must be opened in the Windows Firewall.

Table 13. Port usage for CTI server

Port/Program	Type	Service
5060	TCP/UDP	Recording CTI service
5061	TCP	Recording CTI service
52102	TCP	Recording CTI service

Database Server

Table 14 lists the ports on the Database server that must be opened in the Windows Firewall.

Table 14. Port usage for Database server

Port/Program	Type	Service
1433	TCP	Quality Management SQL database
2303	UDP/TCP	PROXY Pro Gateway service
52103	TCP	DB Proxy service
sqlbrowser.exe	UDP	SQL Server Browser ^a

- a. If the database uses a named instance, sqlbrowser.exe needs to be running and added to the exception list in the firewall. If you are using the default instance (that is, the Instance Name field in QM Databases is empty), you do not need to add sqlbrowser.exe to the firewall exception list.

MediaSense Subscription Server

[Table 15](#) lists the ports on the MediaSense Subscription server that must be opened in the Windows Firewall.

Table 15. Port usage for MediaSense Subscription server

Port/Program	Type	Service
59104	TCP	MediaSense Subscription service
59105	TCP	MediaSense Subscription service

Monitor Server for Server Recording Deployments Only

[Table 16](#) lists the ports on the Monitor server that must be opened in the Windows Firewall for Server Recording deployments.

Table 16. Port usage for Monitor server for Server Recording deployments

Port/Program	Type	Service
59101	TCP	Monitor service

Voice Record Server

If you are not using Windows Firewall, [Table 17](#) lists the ports on the Voice Record server that must be opened.

Table 17. Port usage for Voice Record Server

Port	Type	Service
59102	TCP	Network Recording service
39500-41500	UDP	Network Recording service

If you are using Windows Firewall, [Table 18](#) lists the program on the Voice Record server that must be opened.

Table 18. Port usage for Voice Record Server

Program	Service
VoiceRecordServer.exe	Network Recording service

Site Upload Server

[Table 19](#) lists the ports on the Site Upload server that must be opened in the Windows Firewall.

Table 19. Port usage for Site Upload server

Port/Program	Type	Service
80	TCP	Jetty service (Jetty port)
443	TCP	Jetty service (Jetty SSL port)
2303	TCP	Screen Playback Gateway (PROXY Pro Gateway) service
59100	TCP	Upload Controller service

Recording Methods

Recording Architectures

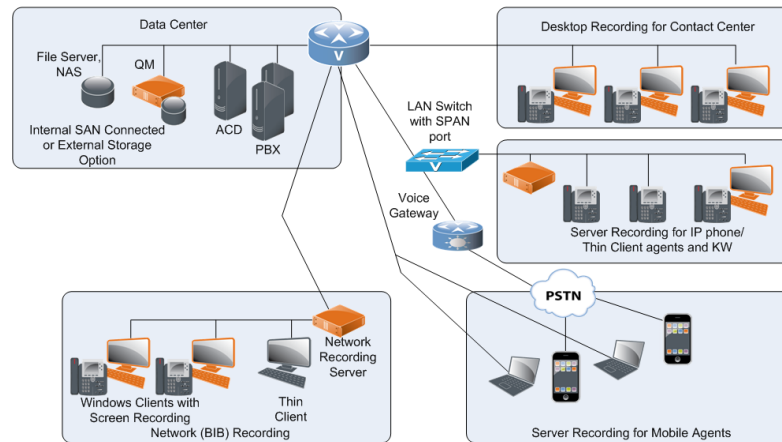
Cisco supports the following recording architectures:

- Agent Recording—all calls go through a PBX or ACD. Call-control signaling tells Quality Management when to start recording and which agent to assign the audio to. Agent Recording supports the following recording methods:
 - Desktop Recording—reliable and scalable in IP-based environments. All audio traffic goes to the agent’s phone regardless of the path it took through the network. All calls are captured from the agent’s perspective. Desktop recording is especially powerful when call center agents are dispersed in various locations because you do not need servers at every location.
 - Network Recording—the preferred option for live voice monitoring. Use Cisco Unified CM to control the phone’s Built in Bridge to fork a call stream for recording or live voice monitoring. All audio traffic goes to the agent’s phone regardless of the path it took through the network. All calls are captured from the agent’s perspective.
 - Server Recording (SPAN)—the preferred option when operating in a thin client environment (for example, Citrix or Windows Terminal Services) in Cisco Unified CCX. All calls go through a switch to reach the agent’s phone. All calls are captured from the switch.
- See [“Agent Recording” on page 50](#) for additional information.
- Gateway Recording—all calls go through a gateway or Session Border Controller (SBC). All calls are captured from the gateway or SBC. Gateway Recording supports the following recording methods:
 - MediaSense Recording—the preferred option for Cisco MediaSense. Cisco MediaSense is a robust scalable clustering architecture. All calls go through and are captured by Cisco MediaSense.

Choose the best architecture for your environment and business needs.

Figure 4. Recording architecture for Cisco

Calabrio Call Recording and Quality Management
for Cisco – Desktop, Server or Network Architecture



Agent Recording

Agent Recording is the use of call-control messages to record calls based on the agent's point of view. The calls are handled by a PBX or ACD.

Cisco supports all of these recording methods along with call-control signaling that tells Quality Management when to start recording and which agent to assign the audio to. The call-control signaling uses JTAPI and SIP messages to determine which agent a call belongs to. Quality Management saves the audio and updates the database with information about the call and associates the call with an agent or user.

The disadvantage of Agent Recording is that even when everything is installed and working properly, calls might not be recorded because of the multitude of configuration and administration options.

Points to remember

For Agent Recording, remember the following points when configuring a load-balanced voice Recording Cluster:

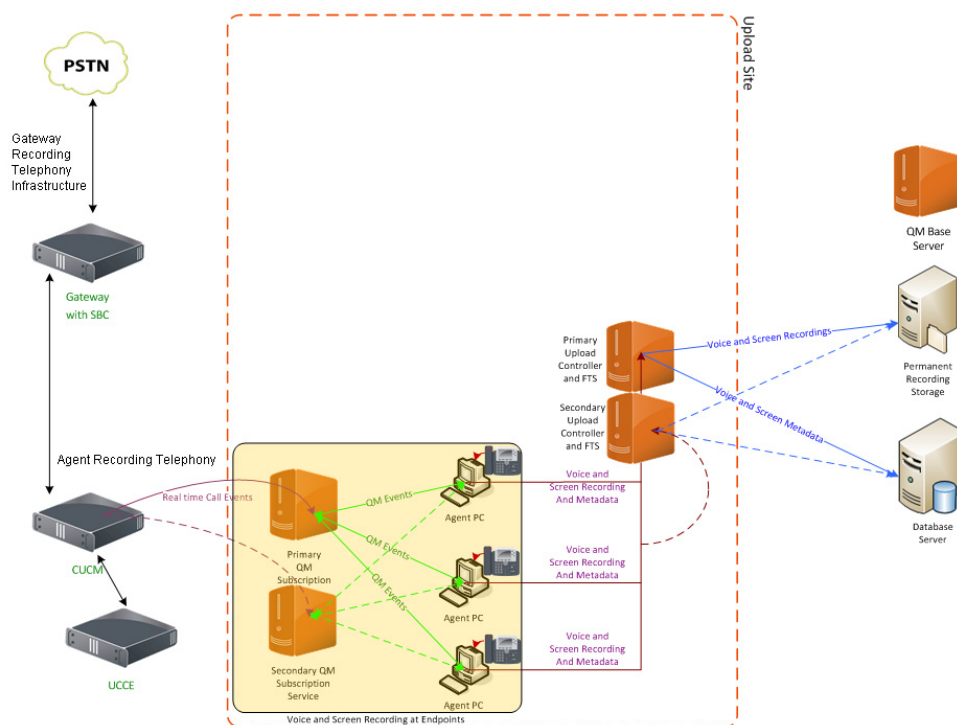
- Device extensions are assigned to a Recording Cluster, not an individual Voice Record Server.
- The load-balancing subscription service is responsible for load balancing recording among all available Voice Record Servers in a Recording Cluster.
- Voice clusters are assigned to a Site Upload server.

- The Voice Record Server only handles voice recording. It does not handle screen recording.
- In a Compliance environment, users are only configured to access recordings.

Desktop Recording (Endpoint) Service Requirements

This section describes the requirements for the Desktop Recording (Endpoint) service.

Figure 5. Desktop Recording



Desktop Recording Considerations

The following deployment scenarios are not supported by the Desktop Recording service. In these instances, you must use Server Recording or Network Recording.

- Thin clients (Citrix or Microsoft Terminal Services)
- Phones without PCs

When you configure your site for Desktop Recording, consider the following:

- The Desktop Recording service does not support SRTP.
- The Desktop Recording service does not support devices with a security profile set to secure in Cisco Unified CM. You must set the security profile to non-secure to record calls using the Desktop Recording service.

Hot Desking

The Desktop Recording service supports hot desking (hoteling) provided the user logs into the computer using their own login ID. Hot desking is one desk shared between several people who use the desk at different times. This work surface can be an actual desk or just a terminal link. Companies where not all the employees are in the office at the same time or not in the office for very long at all regularly use hot desking.

Extension Mobility

Extension Mobility allows the user to log in to the phone so that phone takes on the extension(s) configured for that user. Support for Extension Mobility in a Desktop Recording environment requires the user to log in to a computer with the user's correct Windows NT user name and password. This method assures the correct device is associated with the correct user because the Desktop Recording service can see the phone that is attached to the computer when the user logs in to the computer.

Hard Disk Drive Space on Agent's Computers

Recordings can occupy a great deal of hard disk drive space on an agent's computer. To protect the agent's computer from running out of the free space required for normal operations and to prevent crashes, the Desktop Recording service halts recording when the available hard disk drive space falls below the following minimum capacity:

- Voice recordings—100 MB
- Screen recordings—250 MB

After the space is freed up, recordings will resume.

NOTE: After the recordings are uploaded from the agent's PC to the storage server, the recordings are automatically removed from the PC.

Network Interface Cards

The Desktop Recording service does not function with some network interface cards (NICs). The Intel PRO/100 and PRO/1000 NIC series are unable to detect both voice packets and data packets in a multiple VLAN environment, which prevents the Desktop Recording service from functioning properly. These NICs do not fully support NDIS Promiscuous Mode settings.

A workaround solution is available from the Intel Technical Support website (Solution ID: CS-005897). Another solution is to use a NIC that is fully NDIS-compliant.

The workaround described in CS-005897 might not work for some newer Intel PRO/100 and Intel PRO/1000 cards and drivers.

If the workaround does not solve the problem, the VLAN ID of the IP phone to which the agent computer is directly connected must be added to the VLANs tab of the Intel NIC's Network Connection Properties dialog box.

The IP phone's VLAN ID can be obtained from the phone's Network Configuration screen (press Settings and then choose Network Configuration). For more information, see the documentation specific to your version of the Unified CM and IP phone model.

The following is a partial list of supported NICs:

- D-Link Express Ethernet Workstation Ethernet LAN Connectivity DFE-530TX+
- D-Link Fast Ethernet 10/100Mb Adapter DFE-550TX
- SMC Networks Fast Ethernet PCI Card SMC-1244TX
- SMC Networks EZ Card 10/100 Mbps Fast Ethernet PCI Card SMC-1255TX
- ReadyLINK Express 10/100 Fast Ethernet Adapter RE100TX

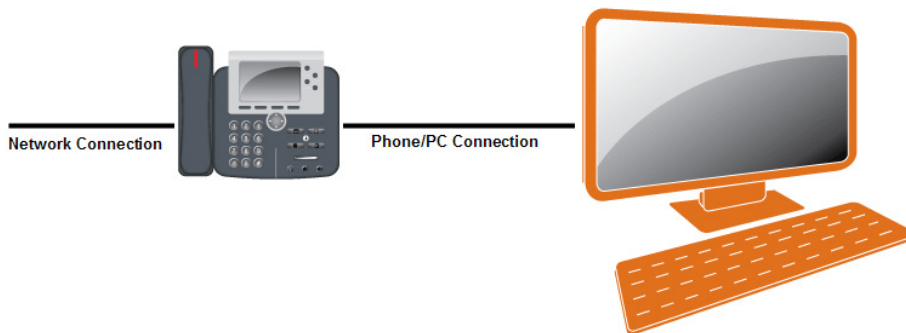
Phone Configurations for the Desktop Recording Service

The Desktop Recording service supports the following phone configurations:

- Hard IP phone and agent computer daisy-chained to the network ([Figure 6](#)). The only time you should daisy-chain your phones is when you intend to use Endpoint Recording or Network Recording.

NOTE: Multiple daisy-chained phones are not supported.

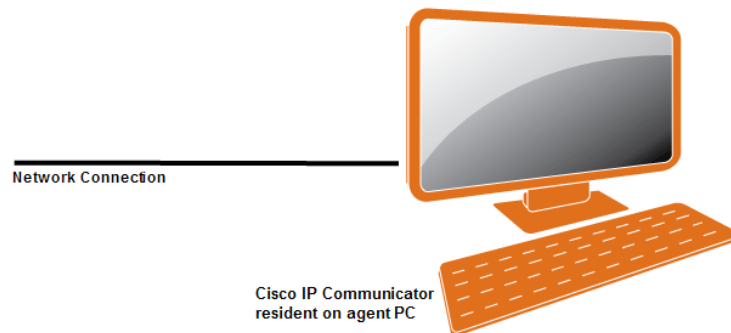
Figure 6. Hardware setup (hard IP phone) for the Desktop Recording service



- Cisco IP Communicator soft IP phone on the agent's computer, connected to the network ([Figure 7](#)). A hard IP phone cannot be on the same network connection as the agent PC. Cisco IP Communicator must be in the computer's startup menu so that it can be detected by the Desktop Recording service.

Information about configuring phones for server recording can be found in the document *Configuring and Troubleshooting VoIP Monitoring*. This document is available on the Cisco website (www.cisco.com).

Figure 7. Hardware setup (Cisco IP Communicator soft IP phone) for the Desktop Recording service



Supported Remote Agent Configurations

Some companies allow their agents to work offsite. You must use a remote agent configuration that is supported by Quality Management.

Hardware VPN Support for Desktop Recording

Quality Management supports Desktop Recording (Endpoint) for remote agents with an attached IP phone or IP soft phone for both voice and screen recording using a Cisco 831 router or the Cisco 871 router.

Software VPN support

Quality Management supports the following VPN software:

- Cisco IP Communicator behind a Cisco Systems VPN Client version 5.0 or later
- Cisco's AnyConnect VPN version 2.5(x) or later
- Check Point VPN

Network Recording

Network Recording uses the Cisco Unified CM Recording functionality to capture voice for recording and the Built-in Bridge (BIB) functionality of capable IP phones to send voice streams from the device being recorded to the Network Recording service. An advantage to the Network Recording approach is that it does not require you to configure SPAN ports for capturing voice traffic.

For more information on this subject, see the "Monitoring and Recording" section of the *Unified CM Silent Monitoring Recording Supported Device Matrix* available at:

<http://developer.cisco.com/web/sip/wikidocs/-/wiki/Main/Unified+CM+Silent+Monitoring+Recording+Supported+Device+Matrix>

When configuring Unified CM Administration for Network Recording, consider the following:

- To enable Network Recording for Quality Management, you must set up Unified CM for Automatic Recording on each line you want to record.
- If you select On Demand for each line you want to record, a third-party application is required to initiate the recording. Quality Management will only capture the voice and screen from the point where a request to record is issued. Quality Management does not initiate the recording. Quality Management does not capture the entire conversation.

When setting up your phones for Network Recording, consider the following:

- Not all IP phones support Network Recording. Phones supported for Network Monitoring and Recording can be found in the *Unified CM Silent Monitoring/Recording Supported Device Matrix* available at:

<http://developer.cisco.com/web/sip/wikidocs>
- A device cannot be configured for Server Recording and Network Recording at the same time. You can, however, change the configuration from Server Recording to Network Recording. Or change a configuration from Network Recording to Server Recording.
- Unlike Server Recording, Network Recording does not act as a backup to Desktop Recording. If a device is configured in Quality Management Administrator for Network Recording, then Network Recording will be the only recording approach used for that device.

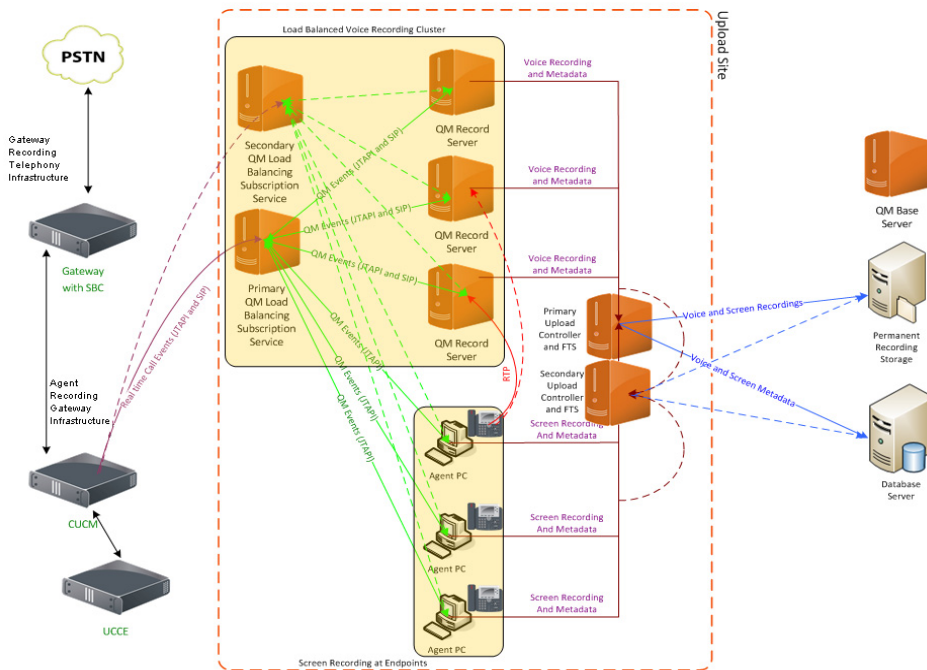
For more information on configuring your system for Network Recording, see the *Administrator User Guide*.

Network Recording supports the recording of Secure Real-time Transport Protocol (SRTP) calls with Cisco Unified CM. See the Cisco Unified CM documentation for more information on configuring SRTP for Quality Management. This includes the configuration of a secure SIP trunk and certificate management. Use the SIP Trunk Certificate tool in System Configuration Setup to configure the certificate required by Cisco Unified CM to establish a trusted relationship for security key exchange. See “[SIP Trunk Certificate](#)” on page 190 for more information.

The Recordings folder for Network Recording is located on same drive where you installed the services for Quality Management.

Cisco recommends using a Redundant Array of Independent Disks (RAID) for storage reliability.

Figure 8. Network Recording



Configuring Cisco Unified CM for Live Voice Recording

Live Voice Recording uses the Unified CM's Silent Call Monitoring feature introduced in Unified CM 6.0 to silently monitor calls. This feature is explained fully in the Cisco documentation. However certain important characteristics of this feature will be repeated here for clarity and to ensure successful configuration, installation and usage.

Remember the following points when configuring phones to support the Live Voice Recording application.

- Live Voice Recording only works on phones or softphones that include a Built-in Bridge (BIB).
- All phones used for live voice monitoring must be set up for Network Recording in both Unified CM Administration and Quality Management Administrator.
- Quality Management only supports Live Voice Recording within a single Unified CM cluster. For example, if a supervisor in cluster A tries to monitor an agent in cluster A, Live Voice Recording is supported. If a supervisor in cluster A tries to monitor an agent in cluster B, Live Voice Recording is not supported.
- Phones used to monitor users do not need to be configured for Network Recording. The extension a supervisor or manager enters in the My Extension field in the Live Voice Recording application must be added to Unified CM

application user group that was configured for Call Monitoring (that is, the Java Telephony API (JTAPI) user) and have a calling search space for the extension that includes the user's line or device partition to allow monitoring the agent.

- Assign the Standard CTI Allow Call Monitoring group to the JTAPI user in Cisco Unified CM. Live Voice Recording requires the permissions provided by this group.
- Live Voice Recording support for Secure calls and multiple codecs is defined by Unified CM. It is not enabled or restricted by Live Voice Recording.
- If a supervisor or manager is configured to be recorded using any recording method (for example, Desktop Recording, Server Recording, or Network Recording), any live voice monitoring sessions they conduct might be recorded. The calls will only be uploaded and displayed as calls in the Quality Management system if they match either an archive workflow or a quality management workflow. To avoid this behavior, an administrator can configure a second extension in Quality Management Administrator, and possibly Unified CM that is not configured to be recorded. Therefore, all calls on the first extension will be recorded, but live voice monitoring sessions conducted on the second extension will not be recorded.
- Unified CM's Silent Call Monitoring feature does not allow multiple supervisors or managers to monitor a single call. As a result, multiple supervisors or managers cannot monitor a single call using the Live Voice Recording application in Workforce Optimization.

Extension Mobility

When configuring agents for extension mobility, you need to ensure the following:

- A user profile is associated with each agent
- Every phone an agent can log in to is associated with a Recording Cluster

When an agent logs in to a phone, their calls are recorded by the Recording Cluster assigned to their phone.

When configuring agents for Extension Mobility, consider the following:

- If the user is on a phone call when they log out of a device, the recording will stop.
- If you change the user profile (for example, the extension) in Unified CM, you must click the Synchronize Devices with Clusters button in the VoIP Devices window for the change to take effect.
- If you change the user profile in Unified CM and synchronize the databases in Quality Management Administrator, current calls on that device might be stopped and restarted.

CTIOS Agent Greeting

We recommend disabling the CTIOS Agent Greeting if you are using Built-in Bridge (BIB). Enabling the CTIOS Agent Greeting with BIB might result in unexpected behavior. For example:

- The CTIOS Agent Greeting was recorded but the recordings are out of sync and garbled.
- The CTIOS Agent Greeting is not recorded.

Supported Remote Agent Configurations

Some companies allow their agents to work offsite. You must use a remote agent configuration that is supported by Quality Management.

Hardware VPN Support for Network Recording

Quality Management supports remote agents with a Network Recording and Monitoring capable IP phone or a Network Recording and Monitoring capable IP soft phone for both voice and screen recording using a router.

Software VPN Support for Network Recording

Quality Management supports Network Recording with Cisco IP Communicator behind a Cisco Systems VPN Client version 5.0 or later.

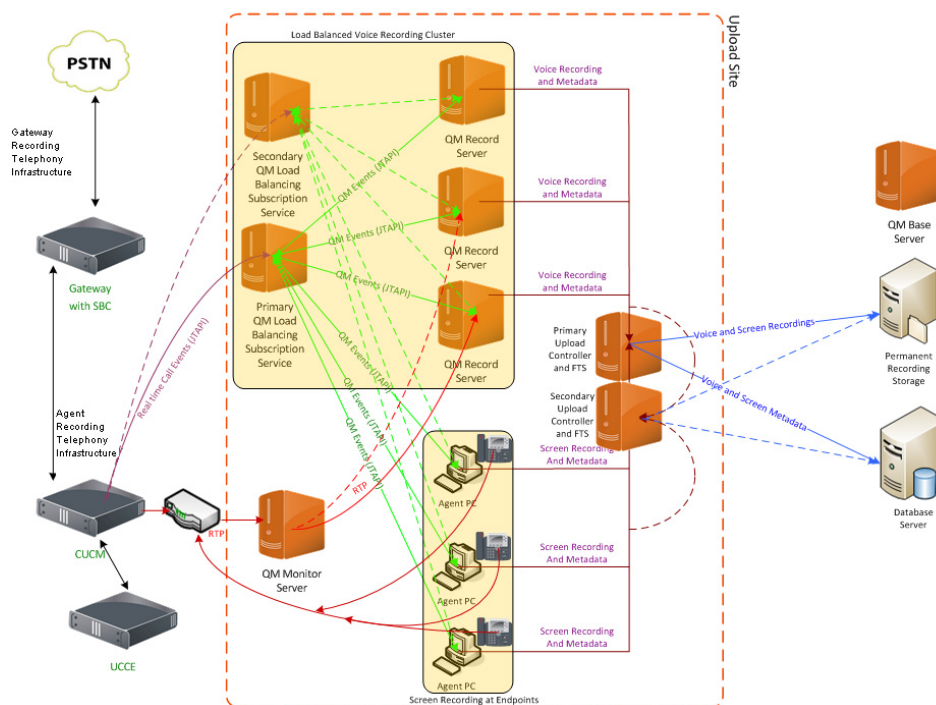
Server Recording (SPAN)

The Cisco Catalyst line of IP network switches support a feature called Switched Port Analyzer (SPAN), or port monitoring, that allows network traffic flowing through a particular switch port or group of ports to be copied and sent to a destination port. The Monitor service listening on this destination port can then get access to packets containing audio data representing a phone call. This method of packet capture is known as Server Recording.

For Server Recording, the Monitor service must be connected to the SPAN port on the switch that is connected to the phones you want to record. See *Configuring and Troubleshooting VoIP Monitoring* for more information on SPAN. This document is available on the Cisco website (www.cisco.com).

The Recordings folder for Server Recording is located on same drive where you installed the services for Quality Management.

Cisco recommends using a Redundant Array of Independent Disks (RAID) for storage reliability.

Figure 9. Server Recording

Configuring Cisco Unified CM for Live Voice Recording

Live Voice Recording uses the Unified CM's Silent Call Monitoring feature introduced in Unified CM 6.0 to silently monitor calls. This feature is explained fully in the Cisco documentation. However certain important characteristics of this feature will be repeated here for clarity and to ensure successful configuration, installation and usage.

Remember the following points when configuring phones to support the Live Voice Recording application.

- Live Voice Recording only works on phones or softphones that include a Built-in Bridge (BIB).
- All phones used for live voice monitoring must be set up for Network Recording in both Unified CM Administration and Quality Management Administrator.
- Quality Management only supports Live Voice Recording within a single Unified CM cluster. For example, if a supervisor in cluster A tries to monitor an agent in cluster A, Live Voice Recording is supported. If a supervisor in cluster A tries to monitor an agent in cluster B, Live Voice Recording is not supported.
- Phones used to monitor users do not need to be configured for Network Recording. The extension a supervisor or manager enters in the My Extension field in the Live Voice Recording application must be added to Unified CM

application user group that was configured for Call Monitoring (that is, the Java Telephony API (JTAPI) user) and have a calling search space for the extension that includes the user's line or device partition to allow monitoring the agent.

- Assign the Standard CTI Allow Call Monitoring group to the JTAPI user in Cisco Unified CM. Live Voice Recording requires the permissions provided by this group.
- Live Voice Recording support for Secure calls and multiple codecs is defined by Unified CM. It is not enabled or restricted by Live Voice Recording.
- If a supervisor or manager is configured to be recorded using any recording method (for example, Desktop Recording, Server Recording, or Network Recording), any live voice monitoring sessions they conduct might be recorded. The calls will only be uploaded and displayed as calls in the Quality Management system if they match either an archive workflow or a quality management workflow. To avoid this behavior, an administrator can configure a second extension in Quality Management Administrator, and possibly Unified CM that is not configured to be recorded. Therefore, all calls on the first extension will be recorded, but live voice monitoring sessions conducted on the second extension will not be recorded.
- Unified CM's Silent Call Monitoring feature does not allow multiple supervisors or managers to monitor a single call. As a result, multiple supervisors or managers cannot monitor a single call using the Live Voice Recording application in Workforce Optimization.

Extension Mobility

When configuring agents for extension mobility, you need to ensure the following:

- A user profile is associated with each agent
- Every phone an agent can log in to is associated with a Recording Cluster

When an agent logs in to a phone, their calls are recorded by the Recording Cluster assigned to their phone.

When configuring agents for Extension Mobility, consider the following:

- If the user is on a phone call when they log out of a device, the recording will stop.
- If you change the user profile (for example, the extension) in Unified CM, you must click the Synchronize Devices with Clusters button in the VoIP Devices window for the change to take effect.
- If you change the user profile in Unified CM and synchronize the databases in Quality Management Administrator, current calls on that device might be stopped and restarted.

Supported Remote Agent Configurations

Some companies allow their agents to work offsite. You must use a remote agent configuration that is supported by Quality Management.

Software VPN Support for Server Recording

Quality Management supports Cisco Systems VPN Client version 5.0 or later in a Server Recording configuration.

Monitoring Server Considerations

When configuring a Monitoring Server for Server Recording, consider the following:

- The Monitoring Server is not supported on a virtual platform. You must run the Monitoring Server on a physical machine.
- The monitor server can handle 200 concurrent calls on a larger server.
- The Monitoring Server must run on its own server that is separate from the Voice Record server.

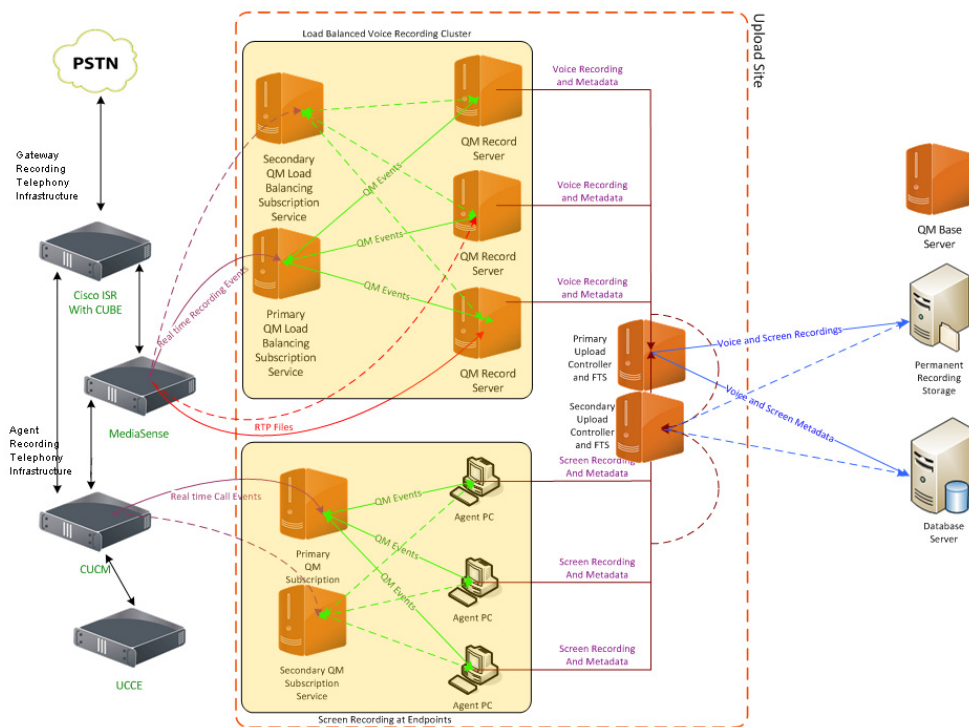
Cisco MediaSense

Cisco MediaSense performs network-based audio and screen recording. Quality Management then imports the MediaSense Recordings to the Recordings application in Workforce Optimization.

The call data for a MediaSense Recording is derived from SIP messages sent to the MediaSense Cluster. The Session Initiation Protocol (SIP) messages are not as rich as JTAPI CTI messages, so some features do not work the same for MediaSense recordings. When a call is placed on hold, the MediaSense recording stops and the raw files are closed. When the call is retrieved from hold, a new set of raw files is created. This means a single call from the agent's perspective can result in multiple call sessions or segments. Quality Management displays each session as a distinct call. Multiple sessions that are logically related (contain the same session ID) will be linked as Associated Calls in the Recordings application. When you play back a MediaSense-recorded call, you must play each of the associated calls to hear the entire call from the agent's perspective.

Recordings persist on Cisco MediaSense. Cisco MediaSense is responsible for the retention and cleanup of recordings on its system.

Figure 10. MediaSense Recording



Cisco MediaSense and Cisco Unified CM

Quality Management supports Cisco MediaSense configured with:

- Cisco Unified CM—see “Unified CCX System Environment” on page 29 for version information.

For more information on Cisco MediaSense, see the *Cisco Unified Contact Center Express (Unified CCX) Software Compatibility Guide* for a complete list of supported combinations. This document is available on the Cisco website (www.cisco.com).

- Cisco Unified CM Built-in Bridge (BIB)—in this configuration, audio forking is done at the agent’s IP phone.

Cisco MediaSense continues Recording when Quality Management is Offline

Under normal operations, Quality Management receives real-time notifications from Cisco MediaSense when call recordings are ready for export.

When the Voice Record Server receives notification, the Voice Record Server immediately exports recordings and metadata from Cisco MediaSense.

If Quality Management is offline, Cisco MediaSense continues to record calls. For example, Cisco MediaSense will record calls under the following circumstances:

- The MediaSense Subscription service or Network Recording service is offline.
- Cisco MediaSense was installed and running in production before Quality Management was purchased and installed.

Quality Management can retrieve these recordings when it returns to an online state so as not to miss any recordings.

MediaSense Clusters

Quality Management supports single and multiple Cisco MediaSense clusters. For more information on Cisco MediaSense configurations, see the following Cisco documents:

- *Installation and Administration Guide for Cisco MediaSense*
- *Solution Reference Network Design for Cisco MediaSense*
- *Release Notes for Cisco MediaSense*
- *Developer Guide Cisco MediaSense*

Redundant Recording with Cisco MediaSense

The Calabrio MediaSense Subscription service can connect with both the MediaSense cluster's primary and secondary API services and will failover when the primary API services fail. The MediaSense Subscription service also includes a synchronization service that allows it to identify and capture any calls recorded by the MediaSense cluster while the MediaSense Subscription service is offline.

Cisco MediaSense implements redundant high availability architecture with Unified CM configured to send recordings to each node in the cluster in succession providing load balancing and redundancy. Recording sessions start with a SIP invite to the node which must respond to the invite within a timeout period or Unified CM will send the SIP invite to the next node in the MediaSense cluster. See the *SRND for Cisco MediaSense* for details.

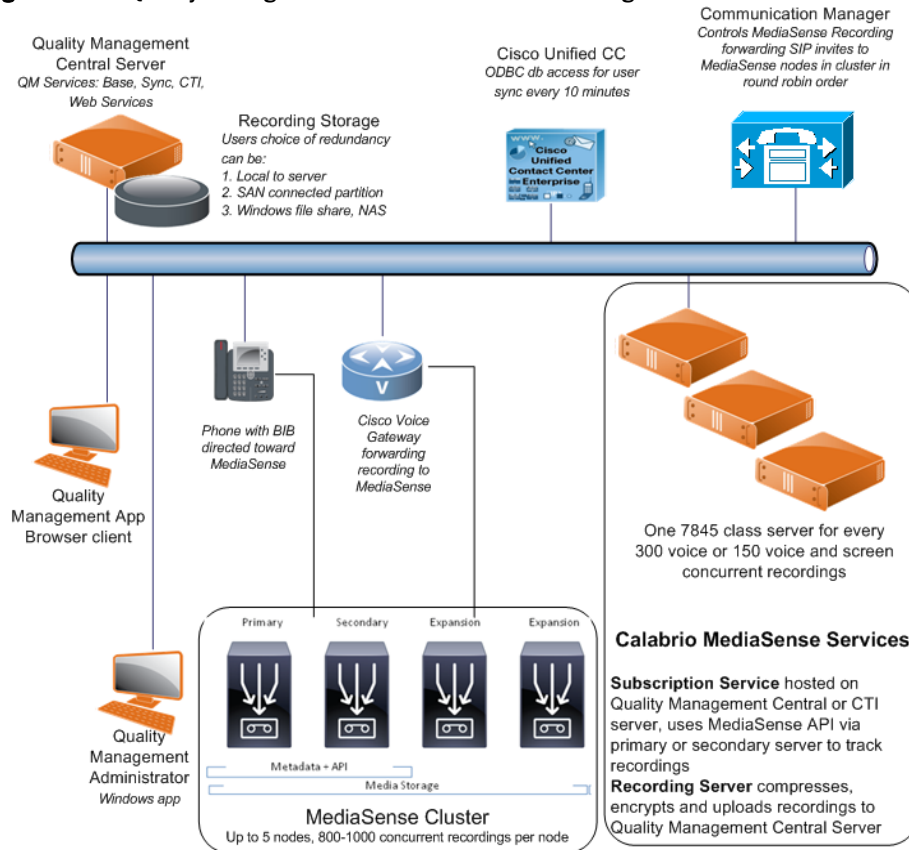
Cisco MediaSense Recording Scalability

Cisco MediaSense Recording uses the following components:

- MediaSense Subscription service—this service is hosted on the Quality Management Base server or CTI server and uses the Cisco MediaSense API through the primary or secondary node to track recordings.

- Voice Record Server—recordings from the MediaSense node are compressed, encrypted, and uploaded to the Voice Record Server. Scalability for MediaSense recording is the same as Network Recording.

Figure 11. Quality Management with MediaSense Recording architecture



Cisco MediaSense Cluster and Scalability

Per the *Solution Reference Network Design for Cisco MediaSense*, each server supports a maximum of 400 concurrent streams. Each call requires two streams, so the server supports a maximum of 200 calls. The MediaSense Subscription service recording upload process for Quality Management also effects scalability by using two streams per call at an accelerated transfer rate equivalent to 5 seconds to upload 60 seconds of the audio recording for a call. This affects the Cisco MediaSense server stream loads as follows:

$$400 \text{ streams per server} = 2 \text{ streams per call} \times (X + X \times (5\text{sec} \div 60\text{sec}))$$

where 5/60 is the recording upload time ratio and X is the number of calls that can be recorded and uploaded concurrently on a continuous basis. For example:

$$X \text{ calls} = 400 \div (2 \times (1 + 5/60)) = 184.61 \text{ concurrent calls}$$

Rounding down with some extra margin results in a concurrent call recording capacity for each Cisco MediaSense server doing immediate uploads of 180 concurrent calls.

If you scale up to a maximum Cisco MediaSense cluster size of 5 servers, the maximum number of concurrent recorded calls per cluster is 900.

Required Codecs

The system environment determines which codecs that Quality Management supports.

Supported Codecs for Unified CCX

[Table 20](#) displays the supported codecs by recording type. You will get a 1KB (8bytes) recording (raw file), if you do not use a supported codec.

Table 20. Supported Codecs by recording type

Recording Type	Codecs		
	G.711	G.722	G.729A
Desktop Recording	x	x	x
Server Recording	x	x	x
Network Recording	x	x	x
MediaSense Recording	x	x	x

NOTE: Quality Management only supports G.729A. It does not support G.729B.

Consult the Unified CM documentation for information on changing the codec of the IP phone.

Shared Lines

Cisco supports shared lines. A shared line is a phone number that is used between two or more IP phones at the same time.

When using shared lines with Cisco MediaSense, Cisco MediaSense will save every recording for each user that has a shared line on their phone. All recordings for each user appear in the Recordings application. The recordings include calls that the user did not answer on the shared line.

When using shared lines, remember the following points:

- Quality Management Monitoring and Recording Services does not support shared lines that call each other when both shared lines are assigned to the same agent (for example, Default Agent)
- Shared lines should be assigned to different agents or the agents should not call each other on those shared lines
- Calabrio Recording Services does not support Hot Desking with shared lines

Supported IP Phones

All phones used by Quality Management for Desktop Recording must support endpoint monitoring. Hard IP phones require a PC port.

See the *Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide* for a list of IP phones that support Desktop Recording, Server Recording, and Quality Management.

See the *Unified CM Silent Monitoring Recording Supported Device Matrix* for a list of IP phones that support Network Recording and Quality Management.

See the *SRND for Cisco MediaSense* for a list of IP phones that support MediaSense Recording and Quality Management.

These documents are available on the Cisco website (www.cisco.com). Not all of the phones listed in these documents are compatible with Quality Management. Phones have to be qualified to work with Quality Management before you install Quality Management.

Supported Phones for Desktop Recording

See “IP Phones for Desktop / Endpoint Monitoring” in the *Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide* for the list of IP phones that support Desktop Recording.

Supported Phones for Server Recording

Any Cisco IP phones that can be controlled by CTI and are connected to a SPAN-enabled switch are supported.

Supported Phones for Network Recording

See the *Unified CM Silent Monitoring Recording Supported Device Matrix* for a list of IP phones that are supported for Network Recording.

Supported Phones for MediaSense Recording

See the *SRND for Cisco MediaSense* for a list of IP phones that support MediaSense Recording.

Cisco IP Communicator Considerations

When configuring phone names for Cisco IP Communicator, consider the following:

- The MAC address for Cisco IP Communicator must not include periods or hyphens.
- For Desktop Recording:
 - The MAC on the client desktop's NIC should be the same configured device name specified in Cisco Unified CM.
 - Running IP Communicator on a desktop or laptop connected to the network through a wireless adapter is not supported.
- For Cisco MediaSense Recording, Network Recording, and Server Recording:
 - Verify all phone names begin with SEP. If the phone names do not begin with SEP, you will not be able to find them when you search for devices from the VoIP Devices window in Quality Management Administrator.

Cisco Jabber

When configuring Cisco Jabber phones for recording, verify the phones' device names in Cisco Unified CM begin with CSF. If the phone names do not begin with CSF, you will not be able to find them when you search for devices from the VoIP Devices window in Quality Management Administrator. Cisco Jabber phone device names usually begin with CSF by default.

NOTE: Cisco Jabber is not supported when using Desktop Recording behind a virtual private network (VPN) connection.

Qualifying Phones for Quality Management

Some phones do not function with the Desktop Recording service. Verify your phones support endpoint monitoring (hard IP phones must have a PC port) before installing Quality Management.

Supported Cisco Unified Outbound Dialer Modes

Quality Management supports the Direct Preview dialing mode.

Resiliency Options

This section describes the options for improving resiliency in your Quality Management environment and covers the following topics:

- [High-level Call Flow](#)
- [CTI and Signaling Services](#)
- [Load Balancing](#)
- [Quality Management](#)

High-level Call Flow

The call flow for Quality Management is as follows:

1. Receive a call.
2. Record voice.
3. Process the workflow.
4. Upload metadata.
5. Upload recordings.

CTI and Signaling Services

Monitoring and Recording Services Quality Management recording can survive when the CTI and signaling services are configured for high availability as follows:

- Unified CM—configure a backup CTI server for your primary CTI server to continue receiving CTI events. See [“Quality Management CTI Service” on page 72](#) for additional information on how the CTI server will behave.

Load Balancing

Prior to version 10.0 or earlier, Quality Management used primary and backup Voice Record Servers to minimize application downtime. Version 10.0 or later uses recording clusters and load balancing to minimize application downtime.

A recording cluster is a group of one or more Voice Record Servers. A Voice Record Server indicates which recording cluster it belongs to when it connects to a load-balancing subscription service.

The load-balancing subscription service will load the recording cluster configuration and register devices assigned to the recording cluster. Calls will be distributed to the Voice Record Servers on a call-by-call basis to the least busy Voice Record Server in the recording cluster.

If one of the Voice Record Servers fails, the load-balancing subscription service will route calls to the remaining Voice Record Servers in the recording cluster.

Quality Management

Quality Management provides a layered approach to call recording resiliency by providing options to add redundancy at multiple layers. The key layers and redundancy options are described in the following topics:

- [Application](#)
- [Quality Management SQL Database](#)
- [Recording Storage Share for Quality Management](#)
- [User Synchronization Service with ACD](#)
- [Call Event Notification](#)
- [Quality Management CTI Service](#)
- [Recording Services](#)
- [Distributed Desktop Recording Services](#)

Application

The Quality Management Base server (primary server) hosts the browser-based user interface, called Workforce Optimization. You can use a standby server (also known as an offline server) to minimize application down time. The standby server is deployed when the primary server fails after restoring the Quality Management SQL database connection and the recording storage share. The standby server assumes the hostname and IP address of the primary Base server to restore communications with user interface and the recording services.

User Licensing

User licensing is maintained in the Cisco Unified CCX CVD license repository. Once the standby server is configured to connect to Unified CCX, the standby server will have access to the same set of licenses as the primary server.

Quality Management SQL Database

The Quality Management SQL database contains the recording metadata required when searching contacts from the Recordings application and the configuration information that is used to enable recording services. Therefore, availability of this SQL database is critical to Quality Management application availability and the uploading of new recordings from the recording services.

There are a variety of SQL database redundancy options available (for example, SQL clustering, redundant storage, and backup and restore). When determining the redundancy option you want to use, consider the following:

- The SQL database host must be available to service the Quality Management requests from either the primary server or the standby server and must have enough capacity to support the Quality Management performance and scaling.
- For high availability, install the SQL database on a separate server from the Base server and use SQL high availability options (for example, clustering to ensure continuous availability).
- If you are using SQL Server clustering, Quality Management database must be installed in a dedicated SQL server instance. No other databases can be installed on this instance.
- Use of point-in-time backup and restore approaches might result in a lack of access to recordings completed between the time of the backup and the restoration of the services for Quality Management. Recordings made during this time might be assigned to duplicate IDs (CCR #) since the restored database would not reflect IDs distributed after the backup. In the case of duplicate IDs, only the first recording uploaded with that ID would be available in the Recordings application, the second recording would be uploaded but not available using a search. Due to this known issue, and other potential problems, an SQL high availability approach such as clustering with high availability storage is recommended.

NOTE: Cisco expects partners and customers to be familiar with Microsoft SQL and the available redundancy options to make their own decisions based on considerations provided here.

Recording Storage Share for Quality Management

A wide variety of Windows file share and/or redundant disk storage options are available. When determining the recording storage share option you want to use, consider the following:

- Recording storage share must be restored and available to the primary or standby server to resume recording upload from the recording services and recording playback from the Recordings application.

- An external high-availability storage solution is recommended over point-in-time backup and restore. The external high-availability storage solution avoids issues with recordings that might upload between the time of the backup and the Base server failure.

NOTE: Cisco recommends that RAID storage solutions include optional battery backup to safely enable write caching, as this generally provides a significant increase in the Input/Output Operations Per Second (IOPS) performance. This is specifically recommended for deployments using Cisco UCS C series servers.

User Synchronization Service with ACD

Quality Management can be configured with redundant ACD connections that will automatically failover to the secondary connection if the primary connection fails.

Call Event Notification

Quality Management relies on receiving the call event feed from Unified CM from the JTAPI interface. QM provides a Cisco Unified CM window in the System Configuration Setup tool that allows the administrator to designate a primary and secondary Unified CM servers within the cluster. When a failure is detected in the CTI feed, Quality Management will automatically failover to the next configured Unified CM.

Quality Management CTI Service

You can deploy a primary and backup Quality Management CTI service on different physical servers. Quality Management software will manage the automatic failover and failback of the CTI service between these services, ensuring the recording services always receive call recording trigger events (for example, start and stop events) which are required for recording.

When using primary and backup CTI services, the CTI services need to be set up in a top-down route list when you configure SIP trunk for Network Recording in Cisco Unified CM. When the primary CTI service goes down, the backup CTI service will start receiving CTI events from Unified CM. See the Cisco Unified CM documentation for more information on configuring a top-down route list.

Recording Services

You should also consider how you deploy some of the supported recording types when you configure your system for redundancy.

Recording Clusters

You can add as many Voice Record Servers to a recording cluster as you want to achieve load balancing and capacity improvements. A recording cluster is a group of one or more Voice Record Servers. A Voice Record Server indicates which recording cluster it belongs to when it connects to a load-balancing subscription service. When using recording clusters, consider the following:

- Recording stops on the Voice Record Server when the Network Recording service or hardware fails. The remainder of the current call is not recorded.
- Recording resumes on the backup Voice Record Server at the start of the next call.

Distributed Desktop Recording Services

The Desktop Recording service is installed and runs on client desktops. The Desktop Recording services leverages the call events from the Monitoring and Recording CTI service to start and stop voice and screen recording on the user's desktop. Since each recorded user has their own independent recording service to record their calls, a Desktop Recording service failure only impacts the single user being recorded by that service. It is expected that the recorded user will move to another functioning phone and desktop, with the Desktop Recording services installed, to resume recording after a failure event.

If the Desktop Recording service cannot connect to the Quality Management database when a user logs in, the user will not be recorded.

Planning Ahead

Because Quality Management works with a variety of operating systems, software, and ACDs, deployment planning is required to ensure that the installation goes smoothly.

Use the information provided here to prepare for Quality Management deployment and installation activities.

Pre-installation and Deployment Checklists

This document provides the following checklists to help the installation go smoothly. The types of checklists are as follows:

- [Pre-Installation Checklists](#)
- [Deployment Checklists](#)

Pre-Installation Checklists

Use the pre-installation checklists to gather configuration information and prepare the servers before you install Quality Management. The pre-installation checklists are as follows:

- [Pre-Installation Checklist](#)
- [Cisco Unified CM Configuration Checklist](#)
- [Cisco Unified CCX Configuration Checklist](#)

Pre-Installation Checklist

Use the following checklist to prepare the customer's site for installing Quality Management.

Table 21. Pre-Installation checklist

Steps	Task	Notes	Done?
Step 1	Complete the QM Express Site Configuration worksheet.	This worksheet allows you to determine storage requirements for the primary recording storage location and the Voice Record Server temporary storage location (optional). This worksheet is available through the Calabrio PDI Help Desk or portal.calabrio.com .	
Step 2	Validate the Quality Management server hardware requirements.	Verify the hardware requirements for the following servers: <ul style="list-style-type: none"> • Base server capacity • Voice Record Server capacity • Monitor server capacity See " Operating Environment " on page 38 for more information on hardware requirements.	
Step 3	Order the server hardware.		
Step 4	Order the Quality Management software and license.		
Step 5	Complete the QM Express Site Configuration worksheet.	This worksheet is available through the Calabrio PDI Help Desk or portal.calabrio.com .	

Table 21. Pre-Installation checklist (Continued)

Steps	Task	Notes	Done?
Step 6	Install the Microsoft Windows Server operating system on the Quality Management server.	<p>For Microsoft Windows Server 2008:</p> <ul style="list-style-type: none"> • Update to the latest service pack (SP) • Verify IIS or Web Services are not enabled (using port 80 or 443) • Disable UAC • Install Desktop Experience—see “Enabling Desktop Experience on Windows Server 2008” on page 87 for instructions on Enabling Desktop Experience. • Install the Telnet client—Optional component for troubleshooting. <p>See “Microsoft Windows Servers” on page 87 for more information on Microsoft Windows Server 2008.</p>	
Step 7	Create the user accounts.	<p>You will need the following user accounts:</p> <ul style="list-style-type: none"> • Local administrator account for installation on the server. • User account to connect to the external storage location—optional. The requirements for this account are as follows: <ul style="list-style-type: none"> – Local administrator – Set permission to run services 	
Step 8	Install the Microsoft SQL Server.	<p>When installing the Microsoft SQL Server:</p> <ul style="list-style-type: none"> • Verify Collation is SQL_Latin1_General_CP1_CI_AS • Verify Mixed Mode Authentication • Create a DBCreator user <p>See “Microsoft SQL Server” on page 88 for information on settings.</p>	

Table 21. Pre-Installation checklist (Continued)

Steps	Task	Notes	Done?
Step 9	Verify all required ports are open to the servers.	See the following topics for more information: <ul style="list-style-type: none"> • “Firewall Requirements” on page 43 • “Adding Firewall Exclusions by Program” on page 90 	
Step 10	Verify the Quality Management software and license files are copied to all Quality Management servers.		
Step 11	Load the Quality Management License on the Cisco Unified CCX server.		
Step 12	Download the latest Quality Management Service Release (SR) from the Cisco website.	This software is available through the Calabrio Portal or portal.calabrio.com .	
Step 12 13	Review the <i>Release Notes</i> .		

Cisco Unified CM Configuration Checklist

Use the following checklist to configure Cisco Unified CM.

Table 22. Cisco Unified CM configuration checklist

Steps	Task	Notes	Done?
Step 1	Associate phones with the JTAPI user.	See “JTAPI User” on page 94 for more information.	

Table 22. Cisco Unified CM configuration checklist

Steps	Task	Notes	Done?
Step 2	Configure Network Recording (optional).	<p>See the Cisco documentation for details.</p> <ul style="list-style-type: none"> • Enable BIB • Create a recording profile for each Voice Record Server • Create a SIP trunk for each CTI Server • Create a route pattern for each Voice Record Server <p>NOTE: Recording redundancy is not supported. Only one SIP trunk can be associated to a route pattern.</p> <ul style="list-style-type: none"> • Set the recording profile on the DN to match the associated Voice Record Server • Configure DN for a monitoring calling search space • Confirm the DN's monitoring calling search space includes a route pattern <p>See “Configuring Cisco Unified CM Administration for Network Recording” on page 99 and <i>Network Recording White Paper</i> for more information on Network Recording.</p>	
Step 3	Verify the phone configuration parameters.	<p>Verify the following parameters for phone configuration are enabled:</p> <ul style="list-style-type: none"> • PC Port • PC Voice VLAN Access • Span to PC Port—Desktop Recording only <p>See “Enabling Required Phone Device Parameters” on page 98 for more information.</p>	

Table 22. Cisco Unified CM configuration checklist

Steps	Task	Notes	Done?
Step 4	Complete the VoIP Device Table tab in the QM Agent List.	This worksheet is only required for MediaSense Recording, Network Recording, or Server Recording. This worksheet is available through the Calabrio PDI Help Desk or portal.calabrio.com .	

Cisco Unified CCX Configuration Checklist

Use the following checklist to configure Cisco Unified CCX.

Table 23. Cisco Unified CCX configuration checklist

Task	Notes	Done?
Set the password for the uccxworkforce user.		

Deployment Checklists

Use the deployment checklists when installing Quality Management and running the System Configuration Setup tool. The deployment checklists are as follows:

- [Server Installation Checklist](#)
- [Configuration Checklist](#)
- [Application Installation Checklist](#)
- [Optional Configuration Checklist](#)
- [Testing Checklist](#)

Server Installation Checklist

Use the following checklist when installing Quality Management components on a single server a single server or multiple servers.

Table 24. Quality Management server installation checklist

Steps	Task	Notes	Done?
Step 1	Install the Quality Management components on the Base server.	See “Install Services on a Single Server” on page 116 for more information.	
Step 2	For a multiple server configuration, install the Quality Management components on the servers.	Install the components on the following servers: <ul style="list-style-type: none"> • Base server • System Database server • Load-balancing Subscription server • Site Upload server See “Install Services on Multiple Servers” on page 117 for more information.	
Step 3	Install the latest SR or ES, if available.	See “Installing a Service Release or Patch” on page 121 for more information on installing an SR or ES.	
Step 4	Complete System Setup Configuration (PostInstall)	Use the information entered in the QM Express Site Configuration worksheet. See “Running System Configuration Setup” on page 125 for more information.	
Step 5	Install any additional servers (optional).	This could include one or more of the following servers: <ul style="list-style-type: none"> • Backup CTI server • Additional Cisco Unified CM Cluster CTI server • Voice Record Server • Monitor server • Monitor server and Voice Record Server 	

Table 24. Quality Management server installation checklist

Steps	Task	Notes	Done?
Step 6	Verify the Screen Playback Gateway (PROXY Pro Gateway) configuration on the Site Upload server.		

Configuration Checklist

Use the following checklist to configure Quality Management from Quality Management Administrator. See the *Administrator User Guide* for more information.

Table 25. Quality Management configuration checklist

Steps	Task	Notes	Done?
Step 1	Configure users.	<ul style="list-style-type: none"> • Link ACD accounts (AD Authentication) or configure ACD accounts (QM Authentication) • Create Quality Management users • Assign roles • License users 	
Step 2	Configure Quality Management teams.	<ul style="list-style-type: none"> • Create teams • Assign knowledge workers • Assign managers 	
Step 3	Configure groups.	<ul style="list-style-type: none"> • Create groups • Assign teams • Assign managers 	
Step 4	Configure evaluation form worksheets.	This is required for QM and AQM licenses only.	
Step 5	Complete the Business Users Worksheet for each workflow.	This worksheet is available through the Calabrio PDI Help Desk or portal.calabrio.com .	
Step 6	Configure evaluation forms.	This is required for QM and AQM licenses only.	
Step 7	Configure workflows.		

Table 25. Quality Management configuration checklist

Steps	Task	Notes	Done?
Step 8	Configure VoIP devices (MediaSense, Server Recording and Network Recording only).	<ul style="list-style-type: none"> • Enable devices for recording • Set recording type • Assign agents to devices or configure devices for Hot Desking • Assign a Voice Record Server • Assign a Monitor server (Server Recording only) 	
Step 9	Configure export settings.		

See the *Administrator User Guide* for more information on configuring Quality Management Administrator.

Application Installation Checklist

Use the following checklist when installing Quality Management applications.

Table 26. Application Installation checklist

Steps	Task	Notes	Done?
Step 1	Install the Recording Thin Client on Citrix servers.	<p>Required only for a Citrix environment.</p> <p>See “Installing Server Applications” on page 193 for more information on installing the Recording Thin Client.</p>	
Step 2	Install the Quality Management Administrator on select workstations.	See “Installing Client Applications” on page 197 for more information.	
Step 3	Install the Desktop Recording service on all PCs that require audio recording or screen recording.		
Step 4	Install the Calabrio Screen Player Plug-in on all PCs used to play back screen recordings.	<p>The Calabrio Screen Player Plug-in requires the AQM license.</p> <p>See “Installing Client Applications” on page 197 for more information.</p>	

Table 26. Application Installation checklist (Continued)

Steps	Task	Notes	Done?
Step 5	Install the latest SR or ES on the client desktop, if available.	See “Installing a Service Release or Patch” on page 121 for more information.	

Optional Configuration Checklist

Use the following checklist when configuring optional features for Quality Management.

Table 27. Optional Quality Management Configuration checklist

Steps	Task	Notes	Done?
Step 1	Configure the Inclusion List.	See “Inclusion List” in the <i>Administrator User Guide</i> .	
Step 2	Configure custom metadata.	See “User-Defined Metadata” in the <i>Administrator User Guide</i> .	
Step 3	Configure Silence and Talk Over events.	See “Call Events Administration” in the <i>Administrator User Guide</i> .	
Step 4	Configure the MANA CDR	See “Monitoring and Notification” on page 174 . This option is not required for MediaSense Recording.	
Step 5	Configure Hot Desking	For Network Recording, MediaSense, or Server Recording: <ul style="list-style-type: none"> • Create a default Hot Desking agent. See the <i>Administrator User Guide</i> for more information. • Install Recording Controls on the Base server. See the <i>API Programmer’s User Guide</i> for more information. 	

Testing Checklist

Log in to Workforce Optimization and use the following checklist to verify Quality Management is running correctly.

See the *Application User Guide* for more information on performing these tasks.

Table 28. Testing checklist

Steps	Task	Notes	Done?
Step 1	Play back an audio recording.	See "Playing Recordings" in the <i>Application User Guide</i> .	
Step 2	Play back a screen recording (AQM).	See "Playing Recordings" in the <i>Application User Guide</i> .	
Step 3	Play back a contact recording.	See "Playing Recordings" in the <i>Application User Guide</i> .	
Step 4	Monitor an active call using the Live Monitoring application (Network Recording only).	See "Live Monitoring" in the <i>Application User Guide</i> .	
Step 5	Run a report.	See "Reporting" in the <i>Application User Guide</i> .	
Step 6	Export a recording.	See "Export Selected Contact" in the <i>Application User Guide</i> .	

Before Installing Quality Management

Read this section and ensure all prerequisites are complete before you install Quality Management.

Microsoft Windows Servers

Microsoft Windows Server Guidelines

Follow these guidelines when installing a Microsoft Windows Server:

- The hostname for the server must not contain underscores if you are using Microsoft Internet Explorer to access the Workforce Optimization Container.
- Cisco only supports the English locale on the server's operating system.
- If a web service is installed on the server, make sure it does not use TCP ports 80 and 443. These ports are used by the Jetty service. See [“Jetty Service Ports” on page 43](#) for more information.
- User Account Control (UAC) must be disabled.

Windows Server 2008

If you are installing Quality Management on Windows Server 2008, you must enable Desktop Experience. Desktop Experience allows the end users to export screen recordings or Windows Media Audio (WMA) from the Workforce Optimization interface.

Enabling Desktop Experience on Windows Server 2008

TASK

1. From the server running Windows Server 2008, choose Start > Server Manager.
2. Click Features, and then click Add Features.

STEP RESULT: The Add Features Wizard appears.

3. Select the Desktop Experience check box, click Next, and then click Install.
4. Reboot the server.

Microsoft SQL Server

Before you install the Quality Management, you must install Microsoft SQL Server 2008 or Microsoft SQL Server 2008 (Express or Standard) either co-resident with the Base server or on an off-board server, and configure it for Quality Management.

All Versions of Microsoft SQL Server

The following topics describe how to install and configure all versions of Microsoft SQL Server for Quality Management.

Installing Microsoft SQL Server

You must install Microsoft SQL Server co-resident on the Base server or on an off-board server, and configure it for Quality Management.

For detailed information about how to install Microsoft SQL Server, see the Microsoft SQL Server installation documentation. When you install Microsoft SQL Server, you must configure the following items as follows:

- Select one of the following options for Instance Name:
 - Default Instance
 - Named Instance. If you choose this option, specify the named instance.
- Under Start Services at the End of Setup, highlight SQL Server and SQL Browser. By default, the SQL Browser Service is set to be started manually, not automatically.

NOTE: If you are using an instance name and not the default instance, you must set the SQL Browser Service to start automatically after you install Microsoft SQL Server.

- Choose Mixed Mode authentication.
- For SQL Collations, select the following option:

Dictionary order, case-insensitive, for use with 1252 Character Set.

NOTE: This option is required to assign the Latin1_General_CP1_CI_AS property to Server Collation in the Server Properties window. See <http://msdn.microsoft.com/en-us/library/ms180175.aspx> for more information.

Microsoft SQL Roles

Create several user logins for the Microsoft SQL Server. For example, you can configure one user login responsible for installation and upgrades and another user login

responsible for day-to-day database activities. For information on creating user logins for Microsoft SQL Server, see the Microsoft documentation.

The user must be configured in SQL Server Management Studio as follows:

- Choose SQL Server Authentication as the authentication mode.
- When entering the password, clear the Enforce Password Policy check box and choose English as the default language.

NOTE: The Quality Management database uses the English date format. If you assign a language other than English to the SQL Server user the language might use a different date format, causing Screen Recording DB errors and Sync errors. The Microsoft SQL Server user must use English as the default language.

- Choose the server roles for the user.
 - For new installations and upgrades, choose the dbcreator check box from the list of server roles. This user is the db_owner of the SQMDB database.
 - For day-to-day database activities, choose the following check boxes from the list of server roles: db_datareader, db_datawriter, and db_owner.

NOTE: If you are upgrading from Microsoft SQL Server 2000 to Microsoft SQL Server 2008 on an existing Quality Management system, also select the db_datareader and db_datawriter server roles.

Microsoft SQL Server Maintenance Plan

The Microsoft SQL Server requires regular maintenance to ensure peak performance. You can automate the maintenance task and schedule it for once a week.

The common database tasks include:

- Check Data Integrity—checks the structural integrity of the data. It verifies the database is not corrupt.
- Reorganize Indexes—moves index pages into a more efficient search order.
- Rebuild Indexes—recreates the indexes with a new fill factor which determines the amount of empty space left in the indexes for future rows.
- Update Statistics—performs sampling of the data in the database to optimize tables and indexes so they can be used more efficiently, increasing performance for the distribution of data in the tables.

IMPORTANT: Do not select the Shrink Database check box when creating a maintenance plan as it might degrade performance in the SQMDB database until it “reaches equilibrium” where DB Cleaner is removing the same number of records as are being added in a normal day. This does not occur until the

system has been running for at least the longest retention time (or 13 months, whichever comes last). Until this point, the database must be allowed to grow.

You can add backups to this schedule if it's appropriate to your business needs. If you have specific requirements for backup, you should probably set up a different maintenance plan that runs on a different schedule (for example, running backups three times a week). See the Microsoft SQL Server documentation for instructions on creating a maintenance plan.

Microsoft SQL Server 2008 Standard and Express Editions

The following topics describe how to complete the configuration of Microsoft SQL Server 2008 for Quality Management.

Microsoft SQL Server 2008 Requirements

If you are using Microsoft SQL Server 2008 you must go to User Account Setup in Windows Server and disable User Account Control (UAC) before you install Quality Management.

NOTE: If you do not disable UAC, you will receive a message indicating Quality Management was unable to save the MSI file when you try to install Quality Management.

Adding Firewall Exclusions by Program

Remote connections require that the Microsoft SQL Server ports are accessible through the firewall. If you use a named instance, then the port that Microsoft SQL Server uses is dynamic so that excluding port numbers in the firewall can be difficult. An easier method is to exclude a program by name.

TASK

1. On the server that hosts Microsoft SQL Server, choose Start > Control Panel > Check Firewall Status.

STEP RESULT: The Windows Firewall application starts.

2. Click Allow a Program or Feature through Windows Firewall.

STEP RESULT: The Allowed Programs window appears, listing all programs on the server.

3. Click the Allow Another Program button.

STEP RESULT: The Add a program dialog box appears.

4. Click Browse and navigate to the Microsoft SQL Server engine.

ADDITIONAL INFORMATION: The path to the Microsoft SQL Server engine is as follows:

- Microsoft SQL Server 2008—C:\Program Files\Microsoft SQL Server\MSQL.10.MSSQLSERVER\MSQL\Binn\sqlservr.exe.
- Microsoft SQL Server 2008 Express Edition—C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS\MSSQL\Binn\sqlservr.exe

If there is more than one instance, “MSQL.10.MSSQLSERVER” or “MSSQL10_50.SQLEXPRESS” might not be the correct instance. Verify that MSQL.10.MSSQLSERVER or MSSQL10_50.SQLEXPRESS is the correct instance before adding Windows Firewall exclusion.

5. Click OPEN.
6. In the Windows Firewall window, verify that sqlservr.exe is in the list of Programs and click Add.

STEP RESULT: All ports that the Microsoft SQL Server 2008 opens are now accessible.

SQL Server Browser

The SQL Server Browser, a Microsoft SQL Server 2008 component, allows a client to search for named instances. By default, the service status for this component is Stopped and the service startup type is Manual. The required service status for the SQL Server Browser is as follows:

- If you are using a default instance, no changes are required for the SQL Server Browser service.
- If you are using a named instance, you need to start the SQL Server Browser service in the Windows Services utility by changing the properties for the service from Manual to Automatic.

Microsoft SQL Server 2008 Express Edition Considerations

If you want to use Microsoft SQL Server 2008 Express Edition in a environment, consider the following Express Edition limitations:

- Supports a maximum of 100 users.
- Supports only 1 CPU (dual/quad cores count as 1).
- Limited to 1 GB RAM. This affects large databases (for example, paging).
- SQL Profiler is not included in the Express Edition. Calabrio’s ability to troubleshoot performance issues will be limited.

Windows SNMP Services

The Simple Management Network Protocol (SNMP) Service adds monitoring capabilities and exposes key information to other computers on your network.

Quality Management uses SNMP to send error messages to specified IP addresses. (You can specify the IP addresses when you run the System Configuration Setup tool.) Install SNMP on the Base server running either Windows Server 2008, or VMware ESX Server.

For more information on using this tool, see the Microsoft SNMP documentation.

SNMP Requirements

- The logged in user must have Administrator privilege or be part of the Administrators group
- Ensure network policies do not prevent installing new Windows services
- The install disk might be required during installation
- These instructions only apply to Windows Server 2008

Installing the Windows SNMP Services on Windows Server 2008

This optional task describes how to install the Windows SNMP services on Windows Server 2008.

TASK

1. On the Quality Management server, select Start > Control Panel and then click Programs and Features.
2. Click Turn Windows Features On or Off.

STEP RESULT: The Server Manager Window appears.

3. Scroll down to Features Summary in the right pane, and then click Add Features.
4. Scroll down to SNMP Services, select the SNMP Services check box, and then click Next.

STEP RESULT: The Confirm Installation Selections window appears.

5. Click Install.

STEP RESULT: A message indicated the installation completed successfully appears.

6. Click Close.

STEP RESULT: The SNMP Service starts automatically: Includes agents that monitor the activity in network devices and reports to the network console workstation.

Configuring SNMP

The following tasks describe how to configure SNMP for Windows Server 2008.

Add the Public Community

TASK

1. Choose Start > Control Panel.

STEP RESULT: The All Control Panel Items appears.

2. Click Administrative Tools.

STEP RESULT: The Administrative Tools window appears.

3. Double-click Services.

STEP RESULT: The Services window appears.

4. Right-click SNMP Services and choose Properties.

STEP RESULT: The SNMP Service Properties window appears.

5. Click the Traps tab, type `public` in the Community Name field, and then click the Add to List button.

STEP RESULT: The Trap Destinations list displays `public` in the list.

6. Click Apply to save your changes.

Configure Security

TASK

1. From the SNMP Service Properties window, click the Security tab.
2. Click the Add button under Accepted Community Names.

3. Choose READ ONLY from the Rights drop-down lists.
4. Type `public` in the Community Name field.
5. Click the Add button, and then click the Apply button to save your changes.

JTAPI User

Quality Management requires that you configure a JTAPI user for Unified CM. This JTAPI user will be used by the Recording CTI service to log in to Unified CM. The JTAPI username and password will be required when you configure Quality Management for Unified CM.

NOTE: If you are configuring Quality Management for Cisco MediaSense Recording, you only need a JTAPI user if you intend to record screen.

To add a JTAPI user for Unified CM, see the “Adding a New User” section in the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager*. This document is available on the Cisco website (www.cisco.com).

When you configure the JTAPI user, consider the following guidelines:

- Quality Management can share the same JTAPI user with other applications (for example, Cisco Unified CCX and Cisco Agent Desktop).
- Assign all devices that you want to record to the JTAPI user.
- Assign the Standard CTI Enabled group to the JTAPI user. You also need to assign the Standard CTI Allow Call Monitoring group to the JTAPI user. Live Monitoring requires the permissions provided by this group.

Active Directory

If your system uses Active Directory, the System Configuration Setup tool prompts you to provide domain information for Active Directory.

Use Active Directory with Quality Management to:

- Allow users to use their existing Windows user name and password to access Quality Management. Using the Windows user name and password eliminates the problem of remembering and maintaining a separate user name and password.

- Enforce password security policies (for example, complexity level or duration), in a single instance across one or more domains.

When a user logs into Workforce Optimization, Quality Management collects the user's username and password. If you configure Quality Management for Active Directory, it sends the login information to the domain's Active Directory server for authentication. When the Quality Management server receives the authentication results, it accepts or rejects the user's access based on the authentication results.

Active Directory Configuration Guidelines

If you are using Active Directory with Quality Management, observe the following guidelines.

- The Quality Management server must be on the same domain as the end users who log in to Workforce Optimization.
- There must be at least one configured domain.
- Each domain must have at least one configured user path.
- If you are using Citrix, set up a recording security group within your Active Directory. A recording security group reduces the number of connections to the server.
- The Quality Management server must be able to access the Active Directory server for user authentication using the port number specified in the Domain Information dialog box in the System Configuration Setup tool. See [“Active Directory” on page 152](#) for more information.

Active Directory Information

Before you install Quality Management, you need the following domain information for Active Directory.

- Base DN
- Domain name—you can locate the Active Directory Domain Name on the machine running Active Directory by right-clicking Active Directory Users and Computers in Administrative Tools, right-clicking the domain folder, and then choosing Properties.
- Active Directory host name or IP address
- Port
- Active Directory display name, password, and user search base
- Admin group—a list of Active Directory users who will be allowed to log into Quality Management Administrator and Workforce Optimization as an administrator.

- User records—for recorded users (agents) and users who will log into Quality Management Administrator and Workforce Optimization as an administrator.

Locating the Active Directory Domain Name

Use this task to locate the Active Directory domain name on the machine running Active Directory. Perform this task only if you are using Active Directory.

TASK

1. Log into the machine running Active Directory.
2. Choose Start > All Programs > Administrative Tools > Active Directory Users and Computers.

STEP RESULT: The Active Directory Users and Computers window appears.

3. Right-click the domain folder and choose Properties.

STEP RESULT: The properties dialog box for that domain appears and displays the domain name in the Domain name (pre-Windows 2000) field.

4. Note the domain name.

ADDITIONAL INFORMATION: The System Configuration Setup tool requires the domain name for Active Directory.

Citrix or Windows Terminal Services

Install Citrix or Windows Terminal Services per the product documentation. When installing Citrix or Windows Terminal Services, use the following settings:

- Servers must include a supported web browser (see the *Desktop Requirements Guide* for web browser requirements) to access the Workforce Optimization Container.
 - Publish the web browser locally to each server.
 - Ensure the security settings allows end users to play back recordings through Citrix or Windows Terminal Services. For more information on security settings, see KB 933991 available at:
<http://support.microsoft.com/kb/933991>
- Each server can support a maximum of 25 concurrent screen recordings.

- Additional configuration settings are required to fully access the Workforce Optimization Container. See the “[Installing Server Applications](#)” on page 193 for complete details.
- Limit the number of simultaneous sessions per user to a single session.
 - For Citrix, follow the instructions at <http://support.citrix.com/proddocs/topic/xenapp5fp-w2k8/ps-sf-connections-limit-v2.html>
 - For Windows Terminal Services, follow the instructions for “Restrict Terminal Services users to a single remote session” at <http://technet.microsoft.com/en-us/library/cc731606%28v=ws.10%29.aspx>

You also need to configure the following settings:

- The Audio Player for Citrix requires the QmWmpAudioPlayer class
- On the server that hosts the Quality Management database, set the dbProperties flag in SQMDB to isCitrix

When these settings are configured, Quality Management supports recording playback with screen.

Citrix Requirements

Quality Management supports Citrix versions 4.5, 4.6, 5.0, 6.5, and XenApp.

External Storage

If you are going to use external storage for voice and screen recordings, you must create a username and password for the external storage user on the external storage server. You will need the username and password when you configure the recording file storage location in the System Configuration Setup tool.

The following services require the external storage user to access the external storage location:

- Jetty service
- Screen Playback Gateway (PROXY Pro Gateway) service

The external storage user must have admin rights to the local system **and** read/write access to the external storage location. The user also needs a right called Log On As Service that allows a service to run as that user. Usually this right has to be added and is not part of the default rights for admin users.

You can assign these rights to the external storage user before you install Quality Management. Go to <http://technet.microsoft.com/en-us/library/cc739424%28v=ws.10%29.aspx> for specific instructions.

If Quality Management is already installed, you can assign these rights to the external storage user by following the instructions above or by manually configuring the service to log in as the external storage user described in “External Storage and Services” on page 191.

Cisco Unified CM

Install Cisco Unified CM per the Cisco documentation.

Follow these guidelines when installing Cisco Unified CM:

- Ensure the following required phone device parameters are enabled in Cisco Unified CM Administration:
 - PC Port
 - PC Voice VLAN Access
 - Span to PC Port—Desktop Recording only

These phone device parameters are enabled by default. You only need to re-enable the parameters if they are disabled.

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

- Create a user in Cisco Unified CM and assign the Administrative XML Layer (AXL) User group to the user. The Quality Management administrator uses this user when:
 - Configuring the SOAP AXL Access and subscriber information in the Cisco Unified CM window
 - Loading the JTAPI jar during System Configuration Setup (PostInstall.exe)
 - Finding devices on the VoIP Devices window in Quality Management Administrator

Enabling Required Phone Device Parameters

For the Desktop Recording service to function correctly, you must enable several required phone device parameters in Unified CM Administration. They are enabled by

default. If for some reason they have been disabled, follow this procedure to re-enable them.

TASK

1. In Unified CM Administration, choose Device > Phone, and then search for and select the agent's phone device.

STEP RESULT: The phone device's Phone Configuration page appears.

2. In the Product Specific Configuration Layout section, set these parameters to Enabled:
 - PC Port
 - PC Voice VLAN Access
 - Span to PC Port—Desktop Recording only

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

3. Click Update.

Configuring Cisco Unified CM Administration for Network Recording

The following instructions explain how to configure Cisco Unified CM Administrator for Network Recording.

Steps	Configuration Steps	Related Procedures and Topics
Step 1	Enable IP phone BIB (Built-in Bridge) to allow monitoring and recording.	See "Cisco Unified IP Phone Configuration" in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 2	Add a user for the monitoring and recording application.	See "Application User Configuration" in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 3	Add the user to a user group that allows monitoring and recording.	See "Application User Configuration" and "User Group Configuration" in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Steps	Configuration Steps	Related Procedures and Topics
Step 4	<i>Optional:</i> Configure tones for monitoring and recording.	You can enable a tone to alert parties on the call that they are being monitored or recorded. See “Service Parameters Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 5	Configure DN for a monitoring calling search space.	See “Directory Number Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 6	Enable recording for a line appearance.	See “Directory Number Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 7	Create a recording profile.	See “Recording Profile Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 8	<i>Optional:</i> Create a SIP profile for Recording CTI service.	See “SIP Profile Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 9	Create a SIP trunk that points to the Recording CTI service.	See “Trunk Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 10	Create a route pattern for the Recording CTI service.	See “Route Pattern Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 11	Configure the recorder for redundancy.	See “Trunk Configuration” in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Creating a User in Cisco Unified CM

Create a user in Cisco Unified CM and assign the Administrative XML Layer (AXL) User Group to the user.

The Quality Management administrator uses this user when:

- Configuring the SOAP AXL Access and subscriber information in the Cisco Unified CM window
- Loading the JTAPI jar during System Configuration Setup (PostInstall.exe)

- Finding devices on the VoIP Devices window in Quality Management Administrator

Informix JDBC Driver

You must install the Informix JDBC Driver for Windows operating system before you install Quality Management. You can download the Informix JDBC Driver from:

http://www14.software.ibm.com/webapp/download/nochargesearch.jsp?S_TACT=104CBW71&S_CMP=&s=&k=ALL&pid=&q=jdbc&ibm-search=Search&pf=&b=&qO=

Select Informix JDBC Driver (Informix JDBC Driver for production use) and 3.70.JC7.

When you install the Informix JDBC Driver use the default installation path and settings.

To install the Informix JDBC driver, extract the files from the downloaded TAR file and follow the installation instructions in the `jdbc_qs_en` HTML document located in the `...\quickstart` folder. When you install the Informix JDBC Driver, use the default installation path and settings.

After the JDBC driver is installed, you need to:

1. Specify the path to the `ifxjdbc.jar` file in the Cisco Unified CC Database window in System Configuration Setup (PostInstall.exe). By default, the `ifxjdbc.jar` file is located in the `C:\Program Files\IBM\Informix_JDBC_Driver\lib` folder.
2. Select Tools > Create Database Catalogs to update the existing database.

Cisco Finesse

Cisco Finesse is a next-generation agent and supervisor desktop designed to provide a collaborative experience for the various communities that interact with your customer service organization. It helps improve the customer experience while offering a user-centric design to enhance customer care representative satisfaction as well

Cisco Finesse is a web-based agent desktop that can be customized. It replaces CAD and CTI OS.

See the *CAD and Finesse Integration Guide* for information on integrating Cisco Finesse with Quality Management via the Recording API.

Fully Qualified Domain Name

Quality Management supports Fully Qualified Domain Names (FQDN) or hostnames and IP addresses when configuring the system.

If you choose to use FQDN, observe the following guidelines:

- The hostnames specified for Quality Management must be resolvable by the clients that need to connect to it.

NOTE: The clients do not need to be part of the domain.

- The client desktop must be able to connect to the server using the hostname.
- If the client is using desktop recording, the client must be able to connect to the following hosts:
 - Base server (Jetty service)
 - DB server (Upload Controller service)
 - Voice Record Servers for Server Recording (SPAN)
 - Site Upload server (Upload Controller service, Jetty service, and FTS)
- The administrator needs to connect to the Base server (Jetty service).

Supporting Asian Languages or Unicode Font

If you have user-entered data in Asian characters or Unicode font (for example, a team name, an agent name, or a question), you must install the supplemental language support for East Asian languages or a Unicode font. If you do not install supplemental language support or a Unicode font, the characters do not appear in the Quality Reports when you generate a PDF form. The following languages require supplemental language support.

- Chinese (China)
- Chinese (Taiwan)
- Japanese
- Korean
- Russian

Installing Supplemental Language or Unicode Font Support

TASK

1. From the Base server, choose Start > Settings > Control Panel.

STEP RESULT: The Control Panel window appears.

2. Double-click Regional and Language.

STEP RESULT: The Regional and Language window appears.

3. Click the Keyboards and Languages tab.
4. Click the Install/Uninstall Languages button.
5. Select the Install Display Languages and browse to the language pack, and then follow the prompts to install the fonts.
6. Restart the Base server.

ADDITIONAL INFORMATION: The server might automatically restart after you install the fonts.

7. Open Windows Explorer and go to C:\Windows\Fonts.

STEP RESULT: The Fonts window appears.

8. Select and copy the font you just added.
 - batang.ttc (Russian and Korean)
 - mingliu.ttc (Chinese and Japanese)
 - A Unicode supported font (for example, Calibri)
9. Go to the C:\Program Files\Cisco\WFO_QM\Java\lib\fonts folder and choose Edit > Paste.
10. Restart the Monitoring and Recording Jetty service.

Supporting Asian Languages or the Unicode Font in PDF Reports

If you are using a non-Asian locale or a Unicode font, but want to include Asian characters or a Unicode font in your PDF reports, you must perform the following steps.

NOTE: The HTML and CVS reports automatically display Asian characters and Unicode fonts.

TASK

1. On the Base server, go to the ... \Program Files\Cisco\WFO_QM\Jetty\calabrio-solutions\reports folder and open the properties file associated with your locale (for example, open QMReport_fr.properties if your locale is French).
2. Find encoding= and change it to encoding=UTF-8.
3. Find font=Arial and change Arial to one of the following fonts:
 - batang.tcc (Russian and Korean)
 - mingliu.tcc (Chinese and Japanese)
 - A Unicode supported font (for example, Calibri)

4. Open Windows Explorer and go to C:\Windows\Fonts.

STEP RESULT: The Fonts window appears.

5. Select and copy the font you just added.
 - batang.tcc (Russian and Korean)
 - mingliu.tcc (Chinese and Japanese)
 - A Unicode supported font (for example, Calibri)
6. Go to the C:\Program Files\Cisco\WFO_QM\Java\lib\fonts folder and choose Edit > Paste.
7. Save and exit the properties file.
8. Restart the Jetty service.

Upgrading from Previous Versions

Quality Management supports direct upgrades from the following versions:

- Quality Management 9.0
- Quality Management 8.5(2)

Upgrades from all other versions are indirect as per the upgrade paths shown in [Table 29](#).

Table 29. Upgrade path

9.0, 8.5(2)	Uninstall the existing Quality Management from the Base server, then install Quality Management 10.0(1). Upgrade client applications over-the-top.
8.5(1)	Upgrade to version 8.5(2). Follow the upgrade instructions in the <i>Monitoring and Recording Services Installation Guide</i> for version 8.5(2).

Before you upgrade, consult the *Release Notes for Cisco Unified Workforce Optimization Quality Management* for any last minute changes to the upgrade procedure.

To upgrade from a previous version, choose one of the options in [Table 29](#), and then complete the upgrade in the following order:

1. Complete the steps in [“Upgrading from Quality Management 8.x\(x\) to 10.0” on page 110](#).
Important: The system you are upgrading to must be running 64-bit Windows Server. Upgrading from a 32-bit Windows Server is not supported.
2. Upgrade the client applications. See [“Upgrading the Client Applications” on page 111](#) for more information on upgrading clients.
3. Test the upgrade on the client machines. See [“Testing the Upgrade on Client Desktops” on page 112](#) for more information on testing the upgrade on client machines.
4. Verify the upgrade is installed correctly. See [“Verifying the Upgrade is Installed Correctly on the Server” on page 113](#) for more information in testing installation.

Automated Update Feature

When upgrading from 8.5(1) or earlier, the Automated Update feature always runs, even if it is disabled. Port changes in 8.5(2) or later requires Quality Management to enable the Automated Update feature because client desktops cannot connect to Quality Management to get the true update flag and run the Automated Update feature.

Proxy Host

When upgrading the Desktop Recording service or the Recording Thin Client software to the latest version, the Proxy Host might be missing. To restore the Proxy Host, locate the Cisco Unified WFO Quality Management in Programs and Features, right-click the Cisco Unified WFO Quality Management, choose Repair, and follow the prompts.

Mark for Quality Feature

When upgrading from 8.5(2) or earlier, note that the Mark for Quality feature has changed so that it now uses the evaluation form specified by the quality management workflow.

Sites

When upgrading from 8.5(2) or earlier, Quality Management will create a single site and assign the Site Upload server, Upload Controller service, and all defined teams to that site. Peak and off-peak settings will also be moved to the site. Once Quality Management is installed, you can add more sites.

Telephony Groups

Table 30 shows the dialog boxes in the Telephony Groups window that replaced the corresponding windows in System Configuration Setup (PostInstall.exe) and System Configuration when upgrading from 9.0(1) or earlier.

Table 30. Windows replaced by dialog boxes in Telephony Groups

System Configuration Setup (PostInstall.exe) or System Configuration windows for 9.0(1) or earlier	Dialog box in the Telephony Groups window
Cisco Unified CM	Unified CM Configuration
Cisco MediaSense	MediaSense Configuration

Unified CM Configuration

When upgrading from 9.0(1) or earlier you must configure the Unified CM version under SOAP AXL Access on the Unified CM Configuration dialog box in System Configuration Setup (PostInstall.exe).

NOTE: An error message will appear if the Version field is not configured.

If you set the Telephony Signaling Method in 9.0(1) or earlier to:

- Mixed—The following telephony groups will be created:
 - CTI—a Unified CM telephony group with a CTI signal method
 - MediaSense—a MediaSense telephony group with a MediaSense signal method
- CTI—a Unified CM telephony group with a CTI signal method will be created.
- MediaSense—The following telephony groups will be created:
 - CTI—a Unified CM telephony group with a CTI signal method
 - MediaSense—a MediaSense telephony group with a MediaSense signal method

Extend Screen Recording

When upgrading from 9.0(1) or earlier, the Extend Screen Recording option moves from Dropped Event in Classifier Configuration window to the Workflow Administrator window. If you specified multiple classifiers in a workflow, the default value (in seconds) for the Extend Screen Recording option defaults to the highest specified value when you upgrade.

Agent Recording

When upgrading from 9.0(1) or earlier note that there has been some fundamental changes to how recordings are managed.

Screen recording and workflow processing has been removed from the Voice Record Servers to reduce load on the Voice Record Servers. The Voice Record Servers only handle voice recording.

The workflow is now processed on the Base server and screen recording is performed on the client desktop (Endpoint). Moving the screen recording to the client desktop removes host to gateway connection issues. All screen recordings will be uploaded at EOD.

For Agent Recording:

- The workflow is used to determine which screen recordings are uploaded. This reduces network usage by only moving the screen recording once for upload, not twice (stream and upload).
- The Recording CTI service now sends screen recording start/stop signals to either the Desktop Record server or the Screen Record (Thin Client Recording) server.
- Cisco Unified CM SIP is now configured to be sent to the Load Balancing Subscription service instead of the Voice Record Servers.

Cluster Recording

When upgrading from 9.0(1) or earlier, each Voice Record Server is associated with a unique Recording Cluster.

Recordings Folder

When upgrading from 9.0(1) or earlier, the recordings in the daily and staging folders under C:\Program Files\QM\Recordings are moved, renamed, and uploaded. The daily and staging folders are then removed. Future recordings are stored in the Recordings folder until they are uploaded.

Configured Devices

When upgrading from 9.0(1), any devices configured for MediaSense in the VoIP Devices window are removed. The devices do not require additional configuration for MediaSense

Integration Configuration

When upgrading from 9.0(1), note that the following buttons have been moved from the Monitoring and Notification window to the Enterprise Settings window in System Configuration Setup (PostInstall.exe) and System Configuration:

- SMTP Configuration
- SNMP Configuration
- CDR Configuration

If you configured a distribution list for an SMTP configuration in 9.0(1), you must create a new distribution list when you upgrade.

Informix Client Software Development Kit

When upgrading from 9.0(1) or earlier, note that the supported Informix Client SDK changed from 32-bit to 64-bit. You must install the Informix Client SDK for Windows x86_64, 64-bit, version 3.70FC7DE, before you install Quality Management. See [“Informix JDBC Driver” on page 101](#) for more information.

NOTE: If Informix Client SDK for Windows x86_64, 64-bit, version 3.70FC7DE, is not installed, an error message appears when you install Quality Management.

Upgrading from Quality Management 8.x(x) to 10.0

Use the following task to upgrade from Quality Management 8.x(x) to 10.0.

TASK

1. On the Base server, back up your Quality Management database.

ADDITIONAL INFORMATION: You need a clean copy of the database if you intend to downgrade from Quality Management 8.5(x+).

See [“Backing Up the Quality Management Databases” on page 207](#) for instructions.

2. Remove the existing Quality Management.

ADDITIONAL INFORMATION: See [“Removing Quality Management 8.x\(x\) or later” on page 203](#) for instructions.

If you are prompted to reboot the machine to remove the software, click No. This reboot prematurely terminates background installation activities. You can manually reboot the machine before you install the Quality Management upgrade.

3. Manually reboot the server.
4. Install Quality Management 10.0 on the Base server and select the Enable Automatic Updates for All QM Clients check box on the Site Settings window in the System Configuration Setup utility.

ADDITIONAL INFORMATION: Selecting the Enable Automatic Updates for All QM Clients check box ensures that Quality Management automatically updates the client desktops after you install Quality Management 10.0.

See [“Installing Quality Management” on page 115](#) for instructions.

5. Restore the Quality Management database.

ADDITIONAL INFORMATION: See [“Restoring the Quality Management Database” on page 208](#) for instructions.

Upgrading the Client Applications

PREREQUISITE

Verify Java JRE version 1.7 is installed on the client desktops.

NOTE: When upgrading to the latest version of Quality Management from a previous version with a patch installed (for example, 8.0(2) SR1ES2), the upgrade might fail. To work around this problem, ensure the application version registry key is set to the version you are upgrading from, then initiate Automated Update feature.

TASK

1. Install the following applications onto each client desktop.

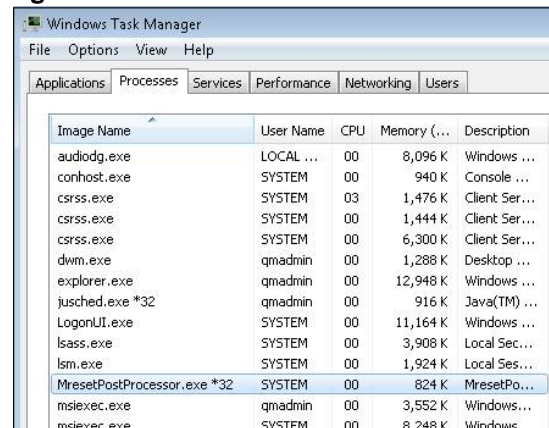
- Calabrio Screen Player Plug-in
- Desktop Recording service
- Quality Management Administrator—on the administrator’s machine only

ADDITIONAL INFORMATION: See [“Installing Client Applications” on page 197](#) for more instructions.

2. Restart the machine when the MRResetPostProcessor is no longer running.

ADDITIONAL INFORMATION: The Process tab Windows Task Manager window ([Figure 12](#)) displays the current CPU status for the MresetPostProcessor.exe.

Figure 12. MresetPostProcessor.exe in the Windows Task Manager window



NOTE: If you are prompted to reboot the machine to complete the installation, click No. This reboot prematurely terminates background

installation activities. You can manually reboot the machine after the MSIPostProcessor DOS window closes.

Testing the Upgrade on Client Desktops

PREREQUISITE

Install the Desktop Recording service on the client desktops if you want to use:

- Screen recording for MediaSense Recording, Network Recording, or Server Recording
- Voice and screen recording for Desktop Recording (Endpoint)

If you have multiple types of client desktops (for example, a laptop with administrator privileges or a desktop with elevated privileges), test three or four of each machine type using Quality Management in your environment and generate test calls to phones associated with each of the client desktops before a scheduled upload occurs.

TASK

1. Log on to a client desktop.
2. Generate test calls.
3. Verify the recordings uploaded successfully to the designated recording file storage location.
4. Repeat steps 1-3 for each client desktop in your test set.
5. After testing the sample client desktops, continue updating the remaining client desktops that have Quality Management installed.

For example, if your environment uses desktops and laptops, you need to test the following scenarios:

- Desktop with administrator privileges
- Desktop with elevated privileges
- Laptop with administrator privileges
- Laptop with elevated privileges

Verifying the Upgrade is Installed Correctly on the Server

Verify Quality Management appears in the list of Add or Remove Programs.

TASK

1. Select Start > Control Panel > Add or Remove Programs or Programs and Features.

STEP RESULT: The services for Quality Management should appear in the list.

2. Verify the version is correct by using one of the following options:
 - For Add or Remove Programs, click Click Here for Support. The version appears in the Support Info dialog box.
 - For Programs and Features, the version appears in the Version column.

Installing Quality Management

When you install Quality Management 9.0, you must choose one of the options in [Table 31](#) and install the components as described.

Table 31. Installing Quality Management

To:	Do This:
Install a single server configuration when no SR is available	<ol style="list-style-type: none"> 1. Install Services on a Single Server. 2. Installing Client Applications.
Install a single server configuration when an SR is available	<ol style="list-style-type: none"> 1. Install Services on a Single Server. 2. Cancel System Configuration Setup. 3. Install a Patch (ES or SR) on the Base server. 4. Manually Run System Configuration Setup on the Base server. 5. Installing Client Applications.
Install a multiple server configuration when an SR is available	<ol style="list-style-type: none"> 1. On the Base server: <ol style="list-style-type: none"> a. Follow steps 1-7 in Install Services on Multiple Servers to install Quality Management. b. Cancel System Configuration Setup. c. Install a Patch (ES or SR) on the Base server. d. Manually Run System Configuration Setup on the Base server. 2. For each additional server: <ol style="list-style-type: none"> a. Follow steps 1-7 in Install Services on Multiple Servers to install the appropriate services. b. Cancel System Configuration Setup. c. Install a Patch (ES or SR) on the server. d. Manually Run System Configuration Setup on the Base server. 3. Installing Client Applications.

Services for Quality Management

Install the services for Quality Management according to your system architecture. See *Integration Guide* for more information.

System Configuration Setup runs automatically after you have installed a service or group of services. When using System Configuration Setup, you must complete System Configuration Setup after an installation in order for the system to function.

Install Services on a Single Server

TASK

1. Load the installation DVD in the server computer, and then navigate to the DVD in My Computer or Windows Explorer.
2. Double-click the file setup_MonRec_<version><build>.exe to start the installation wizard, where <version> is the version number and <build> is the build number.

STEP RESULT: If the Open - Security Warning dialog box appears, click Run to display the Custom Setup dialog box. The InstallShield Wizard prepares to install Quality Management and the InstallShield Wizard dialog box appears.

3. Click Next.

STEP RESULT: The Custom Setup dialog box appears. You need to install all services that appear in this dialog box. These services will be installed on the server.

4. To select a service, click the icon next to each service's name to display a menu and select This feature will be installed on Local Hard Drive. Repeat this step for each service.

ADDITIONAL INFORMATION: You can change the location where the services will be installed by clicking Change and entering a new path.

NOTE: The default path is C:\Program Files\Calabrio. If you need to change the path, do not specify the root directory (for example, D:\ or E:\). Always include at least one folder in the path (for example, D:\Calabrio).

5. Click Next, and then click Install.

STEP RESULT: A window appears and displays the following statement.

`ATTENTION: This window is part of the Quality Management installation process. Do not close this window, it will self terminate when finished.`

Leave the window open. It will close on its own after you complete System Configuration Setup.

6. Click Finish to complete the installation of services.

ADDITIONAL INFORMATION: If you are prompted to reboot the machine to complete the installation, click No. This reboot prematurely terminates background installation activities. You can manually reboot the machine after the MSIPostProcessor DOS window closes.

STEP RESULT: The services you selected are installed, and System Configuration Setup starts.

AFTER COMPLETING THIS TASK:

1. If an SR is available for Quality Management, install the latest SR. For more information, see [“Installing a Service Release or Patch” on page 121](#).
2. Complete the System Configuration Setup windows. For more information, see [“Run System Configuration Setup” on page 126](#).

Install Services on Multiple Servers

TASK

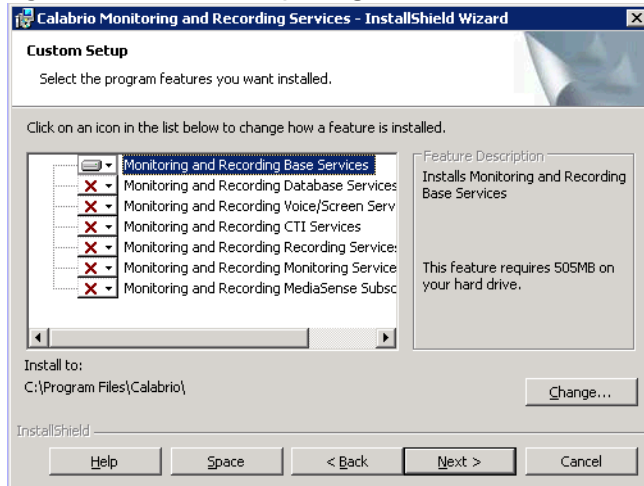
1. Load the installation DVD in the server computer, and then navigate to the DVD in My Computer or Windows Explorer.
2. Double-click the file setup_MonRec_<version><build>.exe to start the installation wizard, where <version> is the version number and <build> is the build number.

STEP RESULT: If the Open - Security Warning dialog box appears, click Run to display the Custom Setup dialog box. The InstallShield Wizard prepares to install Quality Management and the InstallShield Wizard dialog box appears.

3. Click Next.

STEP RESULT: The Custom Setup dialog box appears (Figure 13).

Figure 13. Custom Setup dialog box



4. Select the service or group of services you want to install on this server.

ADDITIONAL INFORMATION: For a multiple server configuration, install Monitoring and Recording Base Services first. You can install the remaining services on the other servers in any order you wish.

Click the icon next to each service's name to display a menu and select This feature will be installed on Local Hard Drive.

You can change the location where the services will be installed by clicking Change and entering a new path.

NOTE: The default path is C:\Program Files\Calabrio. If you need to change the path, do not specify the root directory (for example, D:\ or E:\). Always include at least one folder in the path (for example, D:\Calabrio).

5. Click Next, and then click Install.

STEP RESULT: A window appears and displays the following statement.

`ATTENTION: This window is part of the Monitoring and Recording Services installation process. Do not close this window, it will self terminate when finished.`

Leave the window open. It will close on its own after you complete System Configuration Setup.

6. Click Finish to complete the installation of services.

ADDITIONAL INFORMATION: If you are prompted to reboot the machine to complete the installation, click No. This reboot prematurely terminates background installation activities. You can manually reboot the machine after the MSIPostProcessor DOS window closes.

STEP RESULT: The services you selected are installed, and System Configuration Setup starts.

7. Close the System Configuration Setup window.
8. Repeat [step 1](#) through [step 7](#) for each additional server.

AFTER COMPLETING THIS TASK:

- Complete the System Configuration Setup windows. For more information, see [“Run System Configuration Setup” on page 126](#).

Installing a Service Release or Patch

Periodically, Cisco releases updates. There are several types of updates. The update types are described as follows.

engineering test (ET)

An installable component that contains the files needed to assist developers when diagnosing a problem. An ET is intended for a limited scope test. An ET can contain server and/or client files. Apply the ET on the servers or clients desktops that you want to test. If the ET also contains client files, install the ET directly on the client desktop. The ET does not work with the Automated Update feature.

engineering special (ES)

An installable component that addresses a specific bug fix needed by one or more customers. An ES is cumulative. So, if two ESes are issued against a base release, the second ES contains all the fixes provided in the first ES and new fixes for the current ES. An ES can contain server and/or client fixes. Always install an ES on the Quality Management Base Services server for automatic update to work. An ES is tied to a specific version of the base release and/or Service Release (SR). If the ES contains no fixes for the client side, the Automated Update feature does not update the clients.

You install each ES separately and each ES appears in the Add/Remove Programs window. Separate installation of ESes allows rollback to a previous state. If an ES is server side only, the Add/Remove Program title includes "(Server only)."

service release (SR)

Contains all patches for all bugs found and fixed since the base release of the product. An SR is cumulative. So, if two SRs are issued against a base release, the second SR contains all the fixes provided in the first SR and new fixes for the current SR.

An SR contains fixes for the Quality Management server and/or client desktop. Always install the SR on the Quality Management server. The Quality Management server uses the Automated Update feature, when you enable this feature, to update the clients when you install an SR on the Quality Management Base Services server. If the SR contains no fixes for the client side, the Automated Update feature does not update the clients.

You install each SR separately and each SR appears in the Add/Remove Programs window. Separate installation of SRs allows rollback to a previous state. If an SR is server side only, the Add/Remove Program title includes "(Server only)."

Guidelines for Installing a Patch (SR, ES, or ET)

Use the following guidelines when installing an SR or ES.

- Only one ET can exist on a system at a time. You cannot install an SR or ES until the ET is removed.
- Uninstall any ETs before you install an SR or ES.
- When installing a major, minor, or maintenance upgrade, the ET, ESes, and SRs are automatically removed.
- All but the last ES or SR is uninstalleable. The Remove button is disabled (hidden) for older ESes or SRs.
- When an ET, ES, or SR is uninstalled, the system returns to its previous state.
- A reboot might be required if you uninstall an ET, ES, or SR. A message will appear if a reboot is required.

NOTE: If you are prompted to reboot the machine to complete the removal of the patch, click No. This reboot prematurely terminates background removal activities. You can manually reboot the machine before you run Quality Management.

Install a Patch (ES or SR)

PREREQUISITE

Remove any engineering tests (ET) installed on the server and client desktops. See [“Rolling Back to a Previous State” on page 123](#) for instructions.

Refer to the *Release Notes* for additional installation instructions.

This task provides the basic instructions on installing an engineering special (ES) or service release (SR) on the Quality Management Base server. If the ES or SR includes client-side fixes, and the automatic update feature is available, then the automatic update feature will update the clients.

TASK

1. Download QM_<version number>_SR<number>ES<number_setup>.exe to the Quality Management Base server.
2. Run the executable.

ADDITIONAL INFORMATION: Before installing the SR, the SR checks for any unknown ESes on the Base server. If the SR install finds an unknown ES, the SR install

displays a message and stops the installation process. Uninstall the unknown ES from the Base server and try again.

The same block will happen on the client side whether the automatic update feature is enabled or not. If the SR install finds an unknown ES on the client side, uninstall the unknown ES and try again.

STEP RESULT: The executable installs the files for the SR.

NOTE: If you are installing this SR on a Windows Server 2008, the Files in Use window might appear. Choose Automatically Close and Attempt to Restart Applications, and then click OK.

3. When the System Configuration Setup window appears, complete the fields.
4. Wait five minutes for Jetty to rebuild itself before accessing Workforce Optimization.

Rolling Back to a Previous State

PREREQUISITE

Cisco builds each SR and ES sequentially. When you roll back to a previous state, you must remove the SR or ES in the reverse order they were installed (for example, remove the last SR or ES installed first).

Use this task to remove an SR, ES, or ET installed on the Base server. If you enable the Automated Update feature, Quality Management also removes the SR or ES from the client side to ensure the clients and Base server are in sync with each other. When you remove an SR, ES, or ET, you restore Quality Management to its previous state.

TASK

1. From the Base server, choose Start > Settings > Control Panel.

STEP RESULT: The Control Panel window appears.

2. Double-click Add or Remove Programs.

STEP RESULT: The Add or Remove Programs window appears.

3. Select the SR, ES, or ET that displays “Remove me first” and then click Remove.

ADDITIONAL INFORMATION: If there are multiple patches applied, you must remove the patches in the reverse order they were installed. Always remove the patch that displays a “Remove me first” message first. When you remove the first patch that

displayed this message, the next patch you can remove will now display the “Remove me first” message, and so on. Continue removing patches until you reach the desired state.

To update the Remove Me First, Remove, or Uninstall button in the Add or Remove window when you remove multiple patches, Press F5.

STEP RESULT: The SR, ES, or ET is removed from the Base server.

4. Restart the Jetty service.

Running System Configuration Setup

Use System Configuration Setup (PostInstall.exe) to enter the system configuration information needed for a successful Quality Management installation.

When running System Configuration Setup, remember the following points:

- You must run System Configuration Setup on the computer that hosts the Quality Management server.
- When you run System Configuration Setup for the first time it launches into Initial Mode. When System Configuration Setup runs in Initial Mode:
 - You cannot move forward until you enter all required information.
 - You cannot skip a step.
 - You can go backwards at any time to revisit a previous step.
 - System Configuration Setup saves the text that you entered when you click Next.
 - If a step fails, System Configuration Setup stays at the existing step until the step succeeds or is canceled. The step attempts to run again every time you click Next.
 - Popup dialogs may prompt you for additional information when running in Initial Mode. These popup dialogs provide additional task or tools you must run to fully configure the system. Initial Mode disables the Tools menu. Any time you launch System Configuration Setup thereafter, the System Configuration Setup tool is in Update Mode. Update mode allows you to skip screens and jump around System Configuration Setup. Update Mode enables the Tools menu.
- System Configuration Setup does not display the same windows for each service installation, but only those relevant to that service. You can see different steps depending on your Quality Management configuration.

System Configuration Setup performs the following functions:

- Initially configures the system
 - Configures the location of the servers
 - Configures the connection information for third party software (for example, SQL, ACD, or CTI)
- Performs data upgrade from previous versions of the system
- Provides tools—tasks that typically occur during an installation or upgrade, you may need to complete these tasks outside an installation or upgrade

For more information on the System Configuration Setup interface, see [“System Configuration Setup Interface”](#) on page 132.

Run System Configuration Setup

Complete the System Configuration Setup utility windows as shown in [Table 32](#).

Table 32. System Configuration Setup utility entries

Window or Dialog box	Complete as follows:
	Choose one of the following options: <ul style="list-style-type: none"><li data-bbox="630 785 1378 869">• If you just installed an SR, start System Configuration Setup from the executable PostInstall.exe in C:\Program Files\Cisco\WFO_QM\bin.<li data-bbox="630 890 1378 974">• If you are installing Monitoring and Recording Services Quality Management without an SR, the System Configuration Setup dialog box automatically appears in Initial Mode.
Installation Type	Choose the type of installation you want to perform. Your options are: <ul style="list-style-type: none"><li data-bbox="630 1058 1240 1079">• New Installation—install this version on a new system<li data-bbox="630 1100 1127 1121">• Upgrade—upgrade from a previous version

Table 32. System Configuration Setup utility entries (Continued)

Window or Dialog box	Complete as follows:
System Configuration Setup	<ol style="list-style-type: none"> 1. Choose the network address type. Your options are: <ul style="list-style-type: none"> • IP Address—the IP address of the Base server • Host Name—the FQDN or hostname of the Base server 2. Enter the IP address or hostname of Base server. The Base server is the computer where you installed the Base Services, Database Services, Voice/Screen Services, and Load-balancing Subscription service. 3. Enter the IP address or hostname of the Workforce Optimization Container. The Workforce Optimization Container is located on the Base server. If you also purchased Workforce Management (WFM) and/or Calabrio Speech Analytics, these products will share this container once they are configured to point to this container. 4. Choose one of the following options: <ul style="list-style-type: none"> • If you are running System Configuration Setup on the Base server, choose the IP address or hostname of the Base server from the Local Services drop-down list, and then click OK. • If you are running System Configuration Setup on a different server, choose the IP address or hostname for the server from the Local Services drop-down list, and then click OK. <p>For example, if you want to run Network Recording on a different server and installed the Network Recording service and Monitor service on that server, choose the IP address for the Voice Record server from the IP Address for Local Services drop-down list. If the computer has multiple NICs, multiple addresses appear in the IP Address for Local Services drop-down list. Choose the IP address used for network traffic.</p>
System Database	<p>Complete the fields and click Next.</p> <p>See “System Database” on page 132 for more information.</p>
Database Exists	<p>If the Database Exists dialog box appears, click OK to upgrade your database.</p> <p>The program upgrades the database and loads default data into the database.</p>
Database Loaded	<p>If the Database Loaded dialog box appears, click OK to dismiss the Database Loaded dialog box.</p> <p>This dialog box appears when the database loads successfully.</p>

Table 32. System Configuration Setup utility entries (Continued)


Window or Dialog box	Complete as follows:
Services Started Successfully	Click OK to dismiss the Services Started Successfully confirmation box.
Choose Temporary Storage Location	Click Open  , navigate to the folder where you want to temporarily store recordings, and then click OK. NOTE: The Choose Temporary Storage Location dialog box only appears if this is a new installation.
Select an ACD	Choose an ACD from the Select an ACD drop-down list and then click OK.
Cisco Unified CC Database	Complete the fields and click Next. See “Cisco Unified CC Database” on page 134 for more information.
Telephony Group	Complete the fields and click Next. See “Telephony Groups” on page 138 for more information.
Active Directory Options	Choose one of the following options from the Active Directory Options drop-down list. <ul style="list-style-type: none"> • Use Active Directory—Choose this option if you want to use Active Directory to authenticate user names and passwords. • Use QM Authentication—Choose this option if you want to use Quality Management to authenticate user names and passwords. <p>The program installs the Cisco JTAPI Client. When finished, the JTAPI Configured Successfully confirmation box appears.</p> <p>NOTE: If the Cisco JTAPI Client does not install correctly. You need to install JTAPI manually. See “Manually Installing the Cisco JTAPI Client” on page 130 for instructions.</p>
JTAPI Configured Successfully	Click OK to dismiss the confirmation box.
Change Administrator Password	Type a password for the administrator in the New password field, type the password again in the Confirm new password field, and then click OK. This password allows the administrator to access Quality Management Administrator and Workforce Optimization. The password must be between 1 and 32 characters long. It is case sensitive. NOTE: If you are installing Quality Management for the first time, the Old password field is disabled.

Table 32. System Configuration Setup utility entries (Continued)

Window or Dialog box	Complete as follows:
License Validated Successfully	Click OK to dismiss the License Validated Successfully confirmation box.
Media Server Settings	Click OK to dismiss the Media Server Settings dialog box. The Gateway Administrator window and a new Media Server Settings dialog box appear with instructions on how to configure Screen Playback Gateway.
Site Settings	Complete the fields and click Next. NOTE: Site Settings only appears when you installed the Site Upload Server. If you did not install the Site Upload Server, skip this step. See “Site Settings” on page 164 for more information.
Gateway Administrator	In the Gateway Administrator window, perform the following steps: 1. Choose Local Gateway > Gateway Server > Gateway Security. 2. Click the Click Here to Change Operation Security link. 3. Select the Record to File and Connect to File check boxes in the Allow column, and then click OK.
Gateway Security	If you are using Windows Server 2008, complete the following steps under each tab in Gateway Security: NOTE: If you are not using Windows Server 2008, skip this task. 1. Click Add and enter the name of the user that Quality Management will use to connect for screen playback. If you are using external storage, enter the domain user entered for external storage. If you are using local storage, enter RemoteControlGateway, and then click the Check Name button. 2. Select all check boxes under the Allowed column (the Special Permissions check box is disabled and cleared). 3. Complete step 1 and step 2 for each tab, and then click OK. System Configuration Setup validates the changes. If the changes are incorrect, the Gateway Security dialog box appears again. Correct your changes and try again.
Gateway Administrator	Close the Gateway Administrator window, and then click OK to dismiss the Media Server Settings dialog box.
Inclusion List	Complete the fields and click Next. See “Inclusion List” on page 171 for more information.

Table 32. System Configuration Setup utility entries (Continued)

Window or Dialog box	Complete as follows:
Monitoring and Notification	Complete the fields and click Next. The program generates client information and finishes the System Configuration Setup. See “Monitoring and Notification” on page 174 for more information.
Installation Complete	Click OK to dismiss the confirmation box.
Start Services	Click Yes. The program starts the services for Quality Management. When finished, the Services Started Successfully confirmation box appears.
Services Started Successfully	Click OK to dismiss the confirmation box.
Status	Click Finish to close System Configuration Setup. The Status window shows the versions of all installed Quality Management components. See “Status” on page 183 for more information.

Manually Installing the Cisco JTAPI Client

Follow the instructions in this task only if the System Configuration Setup did not automatically install the Cisco JTAPI Client.

NOTE: This task is not required if you are configuring Quality Management for MediaSense Recording.

TASK

1. Stop the Recording CTI service.
2. Download the Cisco JTAPI Client from the Unified CM Plug-ins webpage.
3. Install the Cisco JTAPI Client on the Quality Management server where the Recording CTI service is installed.
4. Copy the jtapi.jar file from the C:\WINDOWS\java\lib folder to the C:\Program Files\Cisco\WFO_QM\ext folder.

ADDITIONAL INFORMATION: If you are not using the default path to the java\lib folder specified in step 4, copy the jtapi.jar file to correct folder.

5. Start the Recording CTI service.
6. Start System Configuration Setup from the executable PostInstall.exe in C:\Program Files\Cisco\WFO_QM\bin.
7. Choose Tools > Test CTI Service.

STEP RESULT: The CTI Service Ready dialog box appears and displays the following message:

The CTI Service test completed successfully.

8. Click OK to dismiss the dialog box and close the System Configuration Setup window.

System Configuration Setup Interface

Use the System Configuration Setup tool to configure the Quality Management environment. The steps you see in the System Configuration Setup tool depends on the environment in which you install Quality Management and the options that you choose to configure.

System Database

Use the System Database window (Figure 14) to configure connection information for the Quality Management system database (system database).

NOTE: You can only change the information in the System Database window from the System Configuration Setup (PostInstall.exe) or Quality Management Administrator on the Base server. The System Database window in Quality Management Administrator on a client desktop is read-only.

Figure 14. System Database window

Table 33. System Database fields

Field	Description
Host Name/IP Address	<p>The hostname or IP address of the system database server (the server on which SQL Server is installed).</p> <p>If you need to specify a configured port on the system database server, choose Host Name and use the following format in the IP Address field:</p> <p><IP address or hostname>:<port number></p> <p>where <IP address or hostname> is the IP address or hostname and <port number> is the configured port number of the system database server (for example, 10.188.252.11:1455).</p>

Table 33. System Database fields (Continued)

Field	Description
SQL Instance Name	The SQL instance name of the SQL Server. Leave this field blank if you want to use the default instance.
Username	The username used by the DB Proxy service to access the system database. See “Microsoft SQL Server” in the <i>Installation Guide</i> for more information.
Password	The password used by the DB Proxy service to access the system database. See “Microsoft SQL Server” in the <i>Installation Guide</i> for more information.

Configuration Settings Used By Services

If you change the settings on the System Database window, the following table shows when your changes take effect.

Table 34. When services start using the changed configuration settings

Service	Configuration settings applied when...
Data API Service	Restart the service.
DB Proxy Service	Restart the service.
Sync Service	No restart required. The next sync period (every 10 minutes) applies the configuration settings.

Cisco Unified CC Database

Use the Cisco Unified CC Database window (Figure 15) to configure connection information for the Cisco Unified Contact Center Express (Unified CCX) database. Quality Management uses this information to sync agents and teams from Cisco Unified CCX.

Figure 15. Cisco Unified CC Database window

Cisco Unified CC Database

Note: This information is only editable on the Base Server.

Side A

Server Name: qauccx2a

IP Address: 10.192.247.103

Side B

Server Name: qauccx2b

IP Address: 10.192.247.104

DB Instance Name: qauccx2a_uccx

Port: 1504

User: uccxworkforce

Password: *****

ACD Filters

Filters

Sync, Data API, and MANA use the settings in the Cisco Unified CC Database window.

NOTE: You can only change the information in the Cisco Unified CC Database window from the System Configuration Setup (PostInstall.exe) or Quality Management Administrator on the Base server. The Cisco Unified CC Database window in Quality Management Administrator on a client desktop is read-only.

If you are upgrading or modifying Unified CCX, observe the rules provided in [“Rules for Upgrading or Modifying the Unified CC Database in Update Mode”](#) on page 183.

If you modify the information in the Cisco Unified CC Database window after the initial installation and configuration, you must restart the Sync services before your changes take effect.

Table 35. Cisco Unified CC Database fields and buttons

Field	Description
Side A Server Name	<p>The name of the Unified CCX server for the Side A (primary) Cisco Unified CC database.</p> <p>If the server name contains a hyphen (-), replace the hyphen with an underscore (_) when you enter the server name in this field. This ensures the correct configuration of the file name.</p> <p>System Configuration Setup appends _uccx to the name that appears in this field the next time you run System Configuration Setup.</p> <p>NOTE: Do not remove _uccx from the name.</p>
Side B Server Name	<p>The name of the Unified CCX server for the Side B (secondary) redundant Cisco Unified CC database, if one exists.</p> <p>If the server name contains a hyphen (-), replace the hyphen with an underscore (_) when you enter the server name in this field. This ensures the correct configuration of the file name.</p> <p>System Configuration Setup appends _uccx to the name that appears in this field the next time you run System Configuration Setup.</p> <p>NOTE: Do not remove _uccx from the name.</p>
DB Instance Name	<p>The name of the Cisco Unified CCX database. The name is rdsaux01_uccx and the field is disabled by default.</p>
Port	<p>The port number used by the Cisco Unified CCX database. The port number is 1504 and the field is disabled by default.</p>
User	<p>Login ID used to access the Cisco Unified CC database. This user must have write permission to the database. The login ID is uccxworkforce and the field is disabled by default.</p>
Password	<p>Password used by uccxworkforce to access the Cisco Unified CC database.</p>
JDBC Driver	<p>The path to the ifxjdbc.jar file. For example: C:\Program Files\IBM\Informix_JDBC_Driver\lib\ifxjdbc.jar See for “Informix JDBC Driver” on page 101 more information.</p>
Filters	<p>Allows you to determine what data is synced and determines which devices are available in a telephony implementation. See “Touch-Point Filtering” on page 136.</p>

Configuration Settings Used By Services

If you change the settings on the Cisco Unified CC Database window, the following table shows when your changes take effect.

Table 36. When services start using the changed configuration settings

Service	Configuration settings applied when...
Sync Service	<p>No restart is required:</p> <ul style="list-style-type: none"> • After the initial installation • After you fix incorrect sync information <p>The next sync period applies the configuration settings without restarting the Sync service.</p> <p>When there are substantial changes to the database, best practice recommends updating the settings in the Cisco Unified CC Database in the following order:</p> <ol style="list-style-type: none"> 1. Stop the Sync service and the Upload Controller service. 2. Back up the SQMDB catalog. 3. Change the configuration settings on the Cisco Unified CC Database window. 4. Start the Sync service. 5. Verify the data by looking for mass deactivations. 6. Restart the Upload Controller service. Restarting the Upload Controller services adds new calls to the database.
MANA Service	The next polling period applies the configuration settings.
Data API service	Restart the Data API service.

Touch-Point Filtering

Touch-Point Filtering allows you to determine what data is synced and determines which devices are available in a telephony implementation. A “touch point” is a 3rd party system that has data that can be synced with Quality Management for recording purposes. The ability to filter this data so that Quality Management sees only a subset of the touch point’s data is useful in the following environments:

- Multi-tenancy environments where a single ACD/telephony implementation is used by multiple customers and each customer has their own Quality Management installation.

- Environments where an ACD/telephony implementation has more data than Quality Management requires. For example:
 - Only a subset of all extensions are assigned to agents and therefore required for recording purposes.
 - Quality Management will only be used by a subset of the call center.

By default, all teams and users are synced and available to be configured in Quality Management Administrator. Touch-Point Filtering allows you to you to configure filters so that Quality Management only has access to the ACD/Telephony data that matches the filter. The available filters depend on the ACD and telephony implementations.

When you add a filter, the ACD Filter dialog box appears. The fields associated with this dialog box are described in the following table.

Table 37. ACD Filter fields

Field	Description
Name	The name of the ACD filter.
Prefix Type	The type of prefix that Touch-Point Filtering will use to filter the data. In this instance, the data is filtered by Team Name.
Prefix Value	The name of the team. No wildcards are allowed. For example, if you enter Team1, both Team1 and Team10 will be synced.
Trim Prefix	Remove the prefix before adding synced information to Quality Management database. Your options are as follows: <ul style="list-style-type: none"> • True—removes the prefix. True is the default value. • False—keeps the prefix. Example: QM_TeamA becomes TeamA.
Extension Range	The range of extensions that you want to include in the sync.
Device Name Range	The range of devices names that you want to include in the sync.

Telephony Groups

The Telephony Groups window (Figure 16) allows you to add, modify, and delete the following telephony group types:

- Cisco MediaSense clusters
- Unified CM clusters

Figure 16. Telephony Groups window

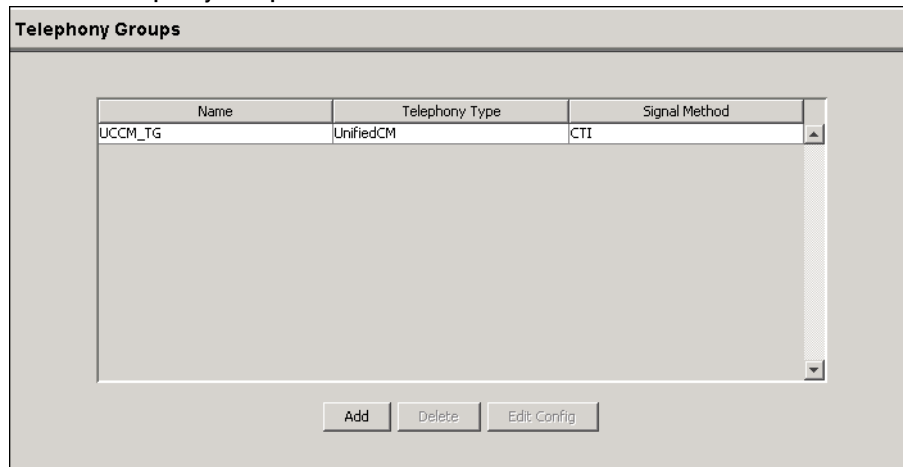


Table 38. Telephony Groups fields

Field	Description
Name	The name of the telephony group.
Telephony Type	The telephony signaling method for Cisco Unified CM. The possible options are as follows: <ul style="list-style-type: none">• UnifiedCM• MediaSense
Signal Method	The telephony signaling method for Cisco Unified CM. The possible options are as follows: <ul style="list-style-type: none">• CTI• MediaSense

Table 39. Telephony Groups buttons

Field	Description
Add	Add a telephony group.
Delete	Delete one or more selected telephony groups.
Edit Config	Modify a selected telephony group.

Telephony Group Configuration

The Telephony Group Configuration dialog box (Figure 17) appears when you add a telephony group. It allows you to assign a name to the telephony group and associate it with a telephony signaling method.

Figure 17. Telephony Group Configuration dialog box

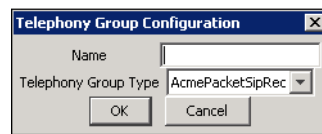


Table 40. Telephony Group Configuration fields

Field	Description
Name	The name of the telephony group. The name must be unique.
Telephony Group Type	The telephony signaling method associated with the telephony group. The possible options are as follows: <ul style="list-style-type: none"> UnifiedCM MediaSense

Unified CM Configuration

The Unified CM Configuration dialog box (Figure 18) appears when you add or edit a telephony group with a Unified CM telephony type. It allows you to configure a Cisco Unified CM cluster.

Figure 18. Unified CM Configuration dialog box

IpAddress	Primary/Backup	Publisher
10.192.252.151	Primary	Publisher

The Cisco Unified CM window also allows you to configure the following users:

- Simple Object Access Protocol (SOAP) Administrative XML Layer (AXL) user
- Unified CM Java Telephony Application Programming Interface (JTAPI) user

These users are used by the Computer Telephony Integration (CTI) service to log in to Unified CM.

A Unified CM cluster has one or more CTI Managers. The CTI Manager is a service that runs on Unified CM and handles JTAPI events for every Unified CM in the cluster. You can specify a primary and backup CTI Manager.

You can specify a primary and backup CTI Manager through Quality Management. Any Unified CM that has the CTI Manager running on the subscriber can be your primary or backup CTI Manager.

NOTE: You can configure any machine as the primary CTI Manager, but it is a good idea to avoid using the publisher, because it already

has the highest load. Using another server as the primary CTI Manager helps avoid decreasing the Unified CM performance.

You can specify one or more Unified CM telephony groups.

NOTE: A Unified CM telephony group requires at least one CTI Manager.

You enter each Unified CM in the Unified CM telephony group in System Configuration Setup so that the Desktop Recording service can find the location of the Recording CTI service. Quality Management stores an association between the Recording CTI service and the Unified CMs in the cluster. If a Unified CM is not in the list, the Desktop Recording service will not know where to register for events.

NOTE: Adding a new Unified CM telephony group here does not actually add a Unified CM cluster. It creates the association between the Recording CTI service and the Unified CMs in the cluster.

Table 41. Unified CM Configuration fields

Field	Description
Name	The name of the telephony group.
Telephony Group Type	The telephony signaling method for Unified CM. The field displays UnifiedCM by default.
Endpoint only does Screen Recording	When selected this check box indicates that the Unified CM telephony group is being used for screen recording only. This only applies when you are using one of the following recording methods: <ul style="list-style-type: none"> MediaSense Recording
Enable Network Recording	When selected this check box indicates that the Unified CM telephony group is using Network Recording and the Recording CTI service will listen for SIP messages. The Recording CTI service will not listen for SIP messages when the check box is cleared.
SOAP AXL Access Username	The AXL (Administrative XML Layer) authentication username for this cluster. The SOAP AXL account is used to access devices in Unified CM from the VoIP Devices window. This username is created when you configure Unified CM.
SOAP AXL Access Password	The AXL authentication password. This password is created when you configure Unified CM.
SOAP AXL Access Version	The Unified CM version. NOTE: An error message will appear if the Version field is not configured.

Table 41. Unified CM Configuration fields (Continued)

Field	Description
JTAPI Username	The JTAPI username for CTI. All phone devices, used for recording are associated with this application user (end user). The Recording CTI service logs into the Unified CM with this user. The username must be between 1 and 32 alphanumeric characters. This field is enabled when you choose CTI or Mixed from the Telephony Signaling Method drop-down list.
JTAPI Password	The JTAPI user's password for CTI. This must be between 1 and 32 alphanumeric characters. This field is enabled when you choose CTI or Mixed from the Telephony Signaling Method drop-down list.
IP Address	The host name or IP address of the subscriber (if any) Unified CMs. You can enter 1 publisher Unified CM, and one or more subscriber Unified CMs. NOTE: When using hostnames, verify the server can resolve the name of the subscribers. If the hostname cannot be resolved, the Recording CTI service cannot log in.
Primary/Backup	The type of CTI Manager. The possible values are as follows: <ul style="list-style-type: none"> • Primary—the primary CTI Manager. There can be only one primary CTI Manager. Once entered, a primary CTI Manager can be reassigned, but not deleted. In a typical configuration, the Primary CTI Manager is a subscriber, not a publisher. • Backup—the backup CTI Manager. There can be one or no backup CTI Manager. • Blank—the CTI Manager is not associated with a primary or backup server. See "Subscriber Configuration" on page 145 for more information.
Publisher	The field indicates whether or not the provided Host Name/IP address is associated with the publisher CTI Manager. If the field is blank, the Host Name/IP address is associated with a subscriber CTI Manager.
CTI Services Primary Host Name/IP Address	The hostname or IP address of the primary Recording CTI service.
CTI Services Backup Host Name/IP Address	The hostname or IP address of the backup Recording CTI service.

Table 42. Unified CM Configuration buttons

Field	Description
Add	Add a new publisher or subscriber. See “Subscriber Configuration” on page 145 for more information.
Delete	Remove the selected publisher or subscriber.
Find Subscribers	Use the AXL user to locate subscribers associated with the publisher entered. This is a good way to validate the AXL user and to populate the list of subscribers, if any are found.

Unified CM Configuration Settings Used By Services

If you change the settings on the Unified CM Configuration window, the following table shows when your changes take effect.

Table 43. When services start using the changed configuration settings

Service	Configuration settings applied when...
Recording CTI Service	Restart the service.
Quality Management Administrator (VoIP Devices)	Reload the VoIP Device window.
Network Recording Service	No restart required. The next polling period applies the configuration settings.
Desktop Recording service	Restart the service.

Adding a Backup CTI Service

This task describes how to add a backup CTI service. The primary CTI service was configured when you installed Quality Management.

TASK

1. From the System Configuration Setup tool on the base machine, choose Telephony Groups.

STEP RESULT: The Telephony Groups window appears.

2. Select a telephony group with UnifiedCM as the Telephony Type and click Edit Config.

STEP RESULT: The Unified CM Configuration dialog box appears.

3. Choose Host Name or IP Address for the CTI Services Backup, and enter the hostname or IP address, and then click OK.
4. Click Next to save your changes.
5. From the backup CTI server, double-click the file setup_MonRec_<version><build>.exe to start the installation wizard, where <version> is the version number and <build> is the build number.

STEP RESULT: The Custom Setup dialog box appears.

6. Click the icon next to the feature named CTI Services and select “This feature will be installed on local hard drive,” from the pop-up menu.

ADDITIONAL INFORMATION: You can change the location where the services will be installed by clicking Change and entering a new path.

7. Click Next, and then click Install.

STEP RESULT: The installation wizard installs the services you selected and starts the System Configuration Setup tool.

NOTE: If Cisco Security Agent (CSA) is running on the server, the installation process stops it temporarily during the installation and restarts it after the installation finishes.

8. Click Next on each window in System Configuration Setup, and then click Finish to complete the installation.

AFTER COMPLETING THIS TASK:

You must restart the Network Recording service for the change to take effect. If you do not restart the Network Recording service, it will not connect to the backup CTI Service.

Subscriber Configuration

Use the Subscriber Configuration dialog box (Figure 19) to add a Unified CM server to the Cisco Unified CM cluster.

Figure 19. Subscriber Configuration dialog box

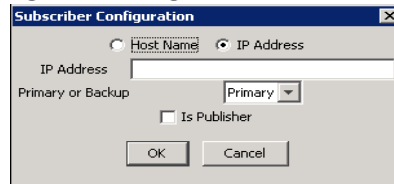


Table 44. Subscriber Configuration fields

Field	Description
Host Name/IP Address	The host name or IP address of the publisher or subscriber (if any) Unified CMs. You can enter up to 8 subscriber Unified CMs. NOTE: When using hostnames, verify the server can resolve the name of the publisher or subscribers. If the hostname cannot be resolved, the Recording CTI service cannot log in.
Primary or Backup	The type of CTI Manager. The options are as follows: <ul style="list-style-type: none"> Primary—the primary CTI Manager. There can be only one primary CTI Manager. Once entered, a primary CTI Manager can be reassigned, but not deleted. In a typical configuration, the Primary CTI Manager is a subscriber, not a publisher. Backup—the backup CTI Manager. There can be one or no backup CTI Manager. Neither—the CTI Manager is not designated as a primary or backup.
Is Publisher	Select this check box if the provided Host Name/IP address is associated with the publisher CTI Manager. Only one publisher CTI Manager is allowed. This check box is disabled when a publisher CTI Manager is configured. NOTE: A publisher CTI Manager must be configured before you can add subscriber CTI Managers.

Subscriber Configuration Settings Used By Services

If you change the settings on the Subscriber Service window, the following table shows when your changes take effect.

Table 45. When services start using the changed configuration settings

Service	Configuration settings applied when...
Recording CTI Service	Restart the service.
Quality Management Administrator (VoIP Devices)	Reload the VoIP Device window.
Network Recording service	Restart the service. NOTE: If you add a backup Recording CTI Service from the System Configuration Setup utility while in Update Mode, you must restart the Network Recording service.
Desktop Recording service	Restart the service.

MediaSense Configuration

The MediaSense Configuration dialog box (Figure 20) appears when you edit a telephony group with a MediaSense telephony type. It allows you to configure the Cisco MediaSense cluster associated with the telephony group. Quality Management uses this information to download call recordings from Cisco MediaSense.

If you modify the information in the Cisco MediaSense window after the initial installation and configuration, you must restart the MediaSense Subscription service before your changes take effect.

Figure 20. MediaSense Configuration dialog box

Table 46. MediaSense Configuration fields

Field	Description
Name	The name of the telephony group.
Telephony Group Type	The telephony signaling method for Cisco MediaSense. The field displays MediaSense by default.
Primary MediaSense API Server IP Address or Hostname	The hostname or IP address of the primary Cisco MediaSense API server.
Secondary MediaSense API Server IP Address or Hostname	The hostname or IP address of the secondary Cisco MediaSense API server.

Table 46. MediaSense Configuration fields (Continued)

Field	Description
MediaSense Subscription Service IP Address or Hostname	The hostname or IP address for the MediaSense Subscription service.
MediaSense Subscription Service Port	The MediaSense port number used by the MediaSense Subscription service. Default = 8440.
Authentication Username	The username for the Cisco MediaSense API server.
Authentication Password	The password for the Cisco MediaSense API server.

MediaSense Configuration Settings Used By Services

If you change the settings on the MediaSense Configuration window, the following table shows when your changes take effect.

Table 47. When services start using the changed configuration settings

Service	Configuration settings applied when...
Monitoring and Recording MediaSense Subscription service	Restart the service.

Enterprise Settings

Use the Enterprise Settings window ([Figure 21](#)) to configure Quality Management.

Figure 21. Enterprise Settings window

The screenshot shows the Enterprise Settings window with the following sections:

- Share Login Fields:** A checkbox labeled "Share login fields with other products." is checked.
- License:** Displays license information: "75 - Compliance Recording (CR) Users", "10 - Quality Management (QM) Users", and "500 - Advanced Quality Management (AQM) Users". Below this is an "Upload License" button.
- Cleanup:** A "Cleanup Time" field is set to "00:05".
- Active Directory:** A table lists domain information:

Domain	Host/IP Address	Display Name
p3	10.192.252.119	rd ldap

 Below the table are "Add", "Remove", and "Edit" buttons.
- Locale:** A dropdown menu is set to "English".
- Integration Configuration:** Three buttons are present: "SMTP Configuration", "SNMP Configuration", and "CDR Configuration". A checkbox "Allow emailing of reports" is checked.
- Session Timeout Options:** Two rows of settings:
 - Desktop (min): 10, with a checked "Unlimited" checkbox.
 - Administrator (min): 10, with a checked "Unlimited" checkbox.

At the bottom, there is a note: "* SMTP and SNMP connection information may only be configured in Post Install on the Base Server". Navigation buttons "Previous" and "Next" are also visible.

NOTE: The Active Directory section appears in the Enterprise Settings window only if your system is configured to use Active Directory.

You can use Enterprise Settings window to do the following:

- Share login fields with other products.
- View license information and update software licenses, if you are not using an ACD, by importing a new software license file.
- Specify when the DB Cleaner service runs.
- Configure Microsoft Active Directory domains (in an Active Directory system only).
- Configure the method (SMTP, SNMP, or CDR) used to notify administrators or supervisors of a system problem
- Configure session time-outs for Call Recording and Quality Management and Quality Management Administrator.
- Configure the locale for your system if your version of Quality Management supports other languages in addition to English.

Configuration Settings Used By Services

If you change the settings on the Enterprise Settings window, the following table shows when your changes take effect.

Table 48. When services start using the changed configuration settings

Service	Configuration settings applied when...
All Clients (Enable Updates change)	Restart the client application.
Quality Management Administrator (AD Authentication and Administrator session timeout change)	Log into Quality Management Administrator.
Workforce Optimization (AD Authentication and localization changes)	Start the Data API service.

Sharing Workforce Optimization with Multiple Products

Workforce Optimization allows you to access several different products from a single login page. You can choose to access all products with a single password or separate passwords for each product when you run the System Configuration Setup tool.

Share Login Fields

You can choose to allow access to one or more of the following products from Workforce Optimization:

- Quality Management
- Calabrio Speech Analytics
- Calabrio Desktop Analytics
- WFM

You can also choose to share common login fields for these products by selecting the Share Login Fields with Other Products check box. If you select this option for each product, users are prompted for a single set of common login credentials.

If a user is not configured for multiple WFO products or the user wants to log into both of the WFO products with different login credentials, the user can select the Separate Product Logins check box in the Login window.

If you do not select the Share Login Fields with Other Products check box, users are prompted for separate login credentials for each WFO product.

Cisco recommends using shared login fields when the users use the same username and password for both products.

See the *Application User Guide* for more information on single-user login authentication.

License

This section displays the available licenses and allows you to import licenses.

What appears in the License section after the initial installation depends on whether the Synchronize Users with ACD check box is cleared or selected. If you select the Synchronize Users with ACD check box, you are running Quality Management with Unified CCX with mixed-mode licensing enabled. Quality Management obtains the licenses from the Cluster View Daemon (CVD) in Unified CCX and then displays the active license information in the License section. Your licenses can be updated through Unified CCX Licensing.

NOTE: If a connection to the CVD cannot be made when initially running System Configuration Setup, Quality Management will continue to try connecting to the CVD. You will not be able to go to the next window until Quality Management can successfully connect to the CVD.

NOTE: If you add new license types (for example, change from only the QM license type to QM and AQM license types), you must ensure Quality Management Administrator is configured to support the new license types (for example, add a quality management workflow and assign users to the AQM license).

Contact your sales representative to obtain a new license file.

Licensing Rules

The license type determines what Quality Management records.

When you log into Workforce Optimization, you have access to all Quality Management applications allowed by the license and roles assigned to you.

The license determines what is recorded, not what is viewed, in Workforce Optimization. For example, if Agents X and Y use AQM or AQMA license, they can record their screens. If the supervisor for these agents only has a QM or QMA license, the supervisor can still view the screen recordings made by these agents.

Importing a License File

This task describes how to import a Cisco CR license file.

TASK

1. Click the Upload License button.

STEP RESULT: The Upload License File dialog box appears.

2. Navigate to the folder where your updated Cisco CR license file is stored, and select the file.
3. Click Upload File.

STEP RESULT: The Licensing Server uploads the Cisco CR license file.

Cleanup

The Database Cleanup Time field specifies when the DB Cleaner utility runs. This utility deletes expired recordings from the database. The value provided must be between 00:00 and 23:59 in 1-minute increments. Choose a time when no uploads are occurring to reduce the load on the system. Default = 00:05.

Active Directory

The Active Directory section appears in the Enterprise Settings window only if your system is configured to use Active Directory. Use the Active Directory section to configure Active Directory domains.

- There must be at least one domain configured
- Each domain must have at least one user path configured

Domain Information

The connection information that you enter for Active Directory in the Domain Information dialog box (Figure 22) is verified using the entered credentials, and the user paths are validated when you click OK in the Domain Information dialog box.

Figure 22. Domain Information dialog box

Table 49. Domain Information fields

Field	Description
Base DN	The location of all Active Directory users in the directory server tree. This field is autofilled with a sample format with variable names that you replace with the domain information. Maximum number of characters allowed = 1000. If your hostname has more than 3 parts, add additional DC= <i>domain</i> statements to the beginning of the Base DN field.
Domain Name	Defaults to the first part of the string entered in the Base DN field. In most cases this is the domain name, but in some cases you must edit the default.

Table 49. Domain Information fields (Continued)

Field	Description
Host Name/IP Address	The host name or IP address of the Active Directory server.
Port	<p>The port used to access the Active Directory server. The field is autofilled with the default port 389, or 636 if you are using SSL (Secure Socket Layer).</p> <p>NOTE: If you change the port to anything other than 389 or 636, clearing or selecting the Use SSL check box will not change the port.</p> <p>The Quality Management server must allow socket communication on this port to be able to access the Active Directory server for user authentication.</p>
Display Name	The name (not the login name, but the display name as configured in Active Directory) of a user with read access to the Active Directory database. Maximum number of characters allowed = 1000.
User Password	The user's password.
User Search Base	The node in the Active Directory folder under which the user resides. Maximum number of characters allowed = 1000.
Use SSL	Select this check box to use SSL for connection to Active Directory. The check box is clear by default and indicates SSL is not enabled. Clearing or selecting this check box changes the default port number in the Port field.
Admin Group	<p>The name of the security group in Active Directory. The users assigned to this security group will be allowed to log in to Quality Management Administrator and Workforce Optimization as an administrator.</p> <p>Best practice: Create a security group with a unique name in Active Directory and add the users who you want to have administrator privileges in Quality Management Administrator and Workforce Optimization. Specify the name of that security group in this field. This prevents any conflict any with default security groups in Active Directory.</p> <p>NOTE: Only users who are a member of this admin group can be an administrator.</p>

Table 49. Domain Information fields (Continued)

Field	Description
User Records (OUs)	<p>One or more paths to user records (OUs). Click Add to add at least one path, or Remove to remove an existing path. Maximum number of characters allowed = 1000.</p> <p>You must specify Active Directory paths from the most specific to the least specific (from left to right in the path statement). For example, if the Active Directory tree is:</p> <pre>ou=US ou=Minnesota ou=Minneapolis ou=Users</pre> <p>Then the user record appears as follows:</p> <pre>ou=Users,ou=Minneapolis,ou=Minnesota,ou=US</pre> <p>Quality Management will search subtrees by default. For example, you could write the user record path as follows, and Quality Management will search all the subtrees under Minnesota.</p> <pre>ou=Minnesota,ou=US</pre>

Table 50. Domain Information buttons

Field	Description
Add Certificate	<p>Locate the Certificate Authority (CA) certificate for Active Directory. Active Directory with SSL requires this certificate. The certificate provides the Active Directory identity and public key for SSL communication.</p> <p>Contact your Active Directory administrator for the location of the CA certificate for Active Directory. In many cases, the Certificate Authority on the Active Directory machine issues the CA certificate for Active Directory. If this is the case, you can access the certificate from:</p> <pre>http://<Active Directory server IP address or hostname>/certsrv</pre> <p>Download the certificate from this website by clicking Download a CA certificate, Certificate Chain, or CRL and save it to a folder. Then click Add Certificate to import the certificate.</p> <p>NOTE: After you import the certificate and save your changes, log out of Quality Management Administrator and log back in to verify the certificate works.</p>
View Certificate	View the certificate associated with Active Directory.
Add	Add a user record.

Table 50. Domain Information buttons (Continued)

Field	Description
Remove	Remove a user record.
Edit.	Modify a user record.
OK	Save your changes.
Cancel	Exit without saving changes.

Managing Active Directory Domains

This task describes how to add or delete an Active Directory domain from the Enterprise Settings window.

TASK

- To add an Active Directory domain, click Add in the Active Directory section. The Domain Information window appears. Complete the fields and click OK.
- To delete an Active Directory domain, select the Active Directory domain you want to delete from the list in the Active Directory section, and then click Remove.

SMTP Configuration

SMTP Configuration allows you to configure the SMTP email connection.

NOTE: This feature is only enabled on the Base server.

Notifications can be sent to either the Event Viewer or in emails to specified recipients. To use email notification, enable the Use Email Notification check box and then configure up to 5 email addresses.

Notification emails will be sent from the sender email address configured in the SMTP Configuration dialog box (Figure 23). If you are using email notification, you must configure SMTP. This can be done only from the Quality Management Base server.

Figure 23. SMTP Configuration dialog box

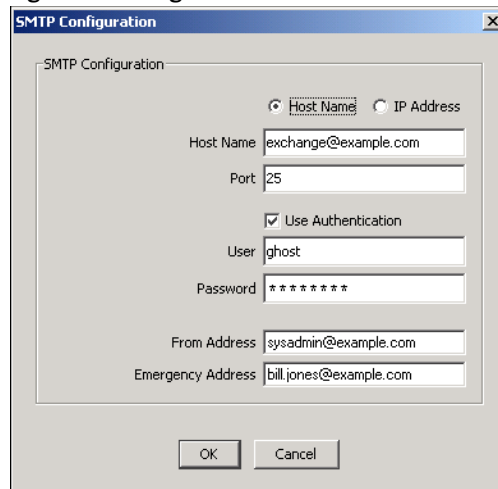


Table 51. SMTP Configuration fields

Field	Description
Host Name/IP Address	Choose Host Name or IP Address, and then enter the hostname or IP address of the SMTP server.
Port	The port used by the MANA service to communicate with the SMTP server.
Use Authentication	Select this check box if authentication is needed to access the SMTP server.
User	The username needed to access the SMTP server.
Password	The password needed to access the SMTP server.
From Address	The email address from which all notifications will come.

Table 51. SMTP Configuration fields (Continued)

Field	Description
Emergency Address	<p>The email address where notification will be sent if the Quality Management database is down when the MANA service attempts to get its initial configuration. The notification email addresses configured in the Monitoring and Notification window are stored in the Quality Management database, and thus will not be functional in the event that the Quality Management database is unavailable when the MANA service first starts.</p> <p>If the MANA service has already obtained a valid configuration from the Quality Management database, and the Quality Management database goes down while the MANA service is running, the MANA service will use the valid configuration it already has. As a result, the notification that the Quality Management database is down will go to the configured email address, not to the emergency address.</p>

Configuring the SMTP Settings for Email

Use this task to configure SMTP settings for email.

TASK

- Click SMTP Configuration, complete the fields, and then click OK.

SNMP Configuration

SNMP Configuration allows you to configure the SNMP connection.

NOTE: This feature is only enabled on the Base server.

Notifications can be sent by Simple Network Management Protocol (SNMP). SNMP is an application-layer protocol that provides a message format for communication between Quality Management and a trap destination.

Figure 24. SNMP Configuration dialog box

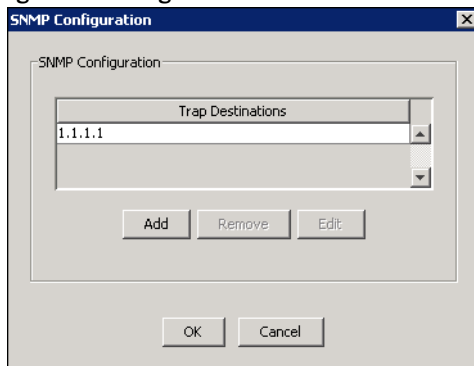


Table 52. SNMP Configuration fields

Field	Description
Trap Destinations	The available trap destinations.

Table 53. SNMP Configuration buttons

Field	Description
Add	Add a trap destination.
Remove	Remove a trap destination.
Edit	Edit a trap destination.

Configuring the SNMP Settings

Use this task to configure SNMP settings for notification.

TASK

- Click SNMP Configuration, choose one of the following options, and then click OK.
 - Click Add to add a new trap destination.
 - Select a listed trap destination and then click Edit to change the IP address.
 - Select a listed trap destination and then click Remove to delete IP address.

AFTER COMPLETING THIS TASK:

Restart the Windows SNMP service to enable your changes.

NOTE: You must restart the SNMP service any time you make a change in trap destinations, including on the initial setup.

CDR Configuration

CDR Configuration allows you to enable the Unified CM's Call Detail Records (CDR) Report.

Figure 25. CDR Configuration dialog box

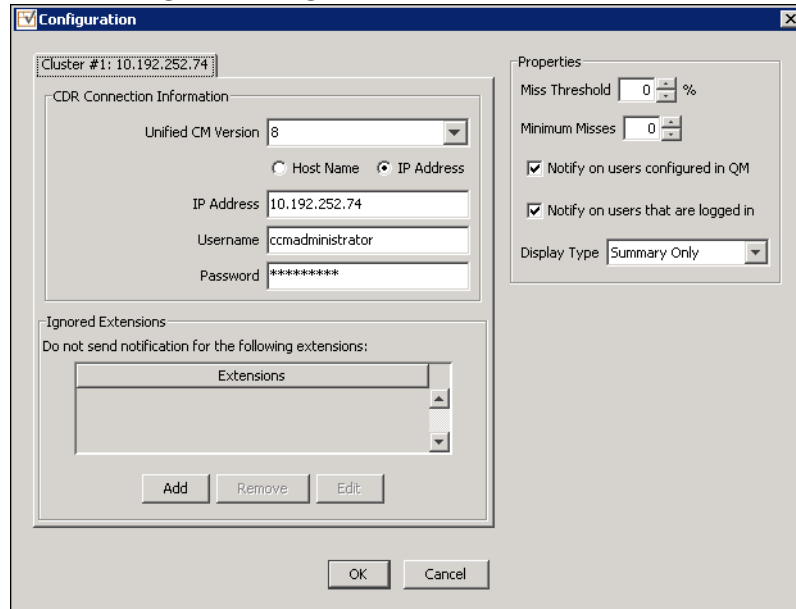


Table 54. CDR Configuration dialog box fields

Field	Description
Cluster <number> <IP address or hostname>	Displays the CDR connection information and ignored extensions associated with the cluster. The number of cluster tabs that appear depend on the number of clusters configured for this system. The fields listed under the Cluster tab applies only to that cluster.
Unified CM Version	Select the version of the Cisco Unified CM you are using.
Host Name/IP Address	Choose host name or IP address, and then enter the information for the Unified CM.
Username	The name of the user with rights to access the CAR reports.
Password	The password of the user with rights to access the CAR reports.

Table 54. CDR Configuration dialog box fields (Continued)

Field	Description
Ignored Extensions	<p>Displays the list of ignored extensions. Quality Management does not send notifications about extensions that appear in this list. Select one of the following options to modify the extensions that appear in this list.</p> <ul style="list-style-type: none"> • Add—add a new extension to the list • Remove—delete an extension from the list • Edit—modify a selected extension in the list

CDR Information Formats for the QM3002 Notification Trigger

You can specify in which format you want to display the CDR information in the CDR Configuration dialog box. Examples of the available formats are listed here.

In these reports, call durations are expressed in milliseconds.

If the agent is listed as “Unknown” it means the agent has not successfully logged in to a PC that has the Desktop Recording service. It is probable that the agent was not configured correctly. Notifications for unknown agents are filtered out if the “Notify on users configured in QM” check box is enabled.

Summary Only

```
Status Report
Start Time: 01/11/2008 15:25:53
End Time: 01/11/2008 16:25:53
Extensions with Missed Calls:
Ext Agent Found Missed % Missed
1545 JonesM 0 8 100%
2201 SmithB 0 15 100%
```

Detail (Tab Delimited)

```
Status Report
Start Time: 01/11/2008 15:23:41
End Time: 01/11/2008 16:23:41
Extensions with Missed Calls:
Ext Agent Found Missed % Missed
1545 JonesM 0 8 100%
2201 SmithB 0 16 100%
Missed Calls (all times in GMT):
CallID Agent Ext ANI DNIS StartTime Duration
16778554 JonesM 1545 2671 1545 01/11/2008 03:29:3613000
16778560 JonesM 1545 2671 1545 01/11/2008 03:29:5214000
16778561 JonesM 1545 2671 1545 01/11/2008 03:30:097000
16778594 JonesM 1545 2671 1545 01/11/2008 03:36:0112000
16778596 JonesM 1545 2671 1545 01/11/2008 03:36:1811000
```

Detail (Plain Text)

Status Report

Start Time: 01/11/2008 15:24:57

End Time: 01/11/2008 16:24:57

Extensions with Missed Calls:

Ext	Agent	Found	Missed	% Missed
1545	JonesM	0	8	100%
2201	SmithB	0	16	100%

Missed Calls (all times in GMT):

Call ID = 16778554

Agent = JonesM

Ext = 1545

ANI = 2671

DNIS = 1545

Start = 01/11/2008 03:29:36

End = 01/11/2008 03:29:49

Duration= 13 sec

Call ID = 16778560

Agent = JonesM

Ext = 1545

ANI = 2671

DNIS = 1545

Start = 01/11/2008 03:29:52

End = 01/11/2008 03:30:06

Duration= 14 sec

Managing Ignored Extensions

TASK

- To add an ignored extension, click Add in the Ignored Extensions section, enter the extension in the field, and then click OK.
- To edit an ignored extension, select the connection you want to edit in CDR connections, click Edit, make the necessary changes in the Edit Extension dialog box, and then click OK
- To remove an ignored extension, select an extension from the Ignored Extensions list and click Delete.

Allow Emailing of Reports

When selected, the Allow Emailing of Reports check box allows you to email a report to a specific person or distribution list. For more information on creating a distribution list, see [“Notification Distribution” on page 178](#).

Session Timeout Options

You can configure Quality Management Administrator or Quality Management in Workforce Optimization for one of the following options:

- Close all open popup windows and log off the user after a specified number of minutes of inactivity (session time-out)
- Allow a user to remain logged in indefinitely (default setting)

To configure the session timeout period, enter the desired number of minutes of inactivity before timeout occurs in the minutes field.

NOTE: When you change the Session Timeout value for Quality Management Administrator, you must restart Quality Management Administrator before the changes can take effect.

If a user accessed one or more Quality Management applications, each application displays a Timeout Warning dialog box 30 seconds before the application actually times out. If the user does not respond to the Timeout Warning dialog box, the dialog box and the application are closed and an alert is sent to the user stating that the application timed out and was closed.

When you are playing a contact recording, the session remains in an active state. Workforce Optimization does not time out when you are playing a contact recording.

Locale

Use the Locale section to enable the default language in the Workforce Optimization interface. Users can change the default language when they log in to Workforce Optimization.

NOTE: The Locale section only appears when multiple locales are available.

Changing the Default Locale

The following task describes how to change the default locale for the Workforce Optimization interface.

TASK

- Select the desired language from the Locale drop-down list.

Site Settings

Use the Site Settings window (Figure 26) to configure one or more sites and associate teams and Recording Clusters with each site.

Figure 26. Site Settings window

The screenshot shows the 'Site Settings' window with the following configuration:

- Delete Selected Site:** [Button]
- Default Site:** Default Site (dropdown)
- Default Site IP:** 10.10.51.148
- Site Name:** Default Site
- Enable automatic updates for all QM clients:**
- Peak Uploads:**
 - Peak Hours Begin: 09:00
 - Peak Hours End: 17:00
 - Max Peak Hour Uploads: 5
 - Max Off Hour Uploads: 100
- Storage Location:**
 - IP Address: 10.192.252.195
 - Local Storage Location External Storage Location
 - Path: \\Program Files (x86)\Common Files\QM\recording [Browse]
 - Username: [Field]
 - Password: [Field]
- Teams:**

Team ID	Team	Site
5000.5047	wfntessteam	10.10.51.148
- Assigned Teams:**

Team ID	Team
5000.5059	zTeam1020
5000.5049	laubewfmsh
5000.5024	CharlieTeam2
5000.5053	laube19
- Recording Clusters:**

Name
2
10
- Assigned Recording Clusters:**

Name
5

[Save] [Cancel]

When you install the Site Upload Server on a server, this is the first screen to appear in System Configuration Setup (PostInstall.exe).

NOTE: The Site Settings window only appears when you install the Site Upload Server.

You can use the Site Settings window to do the following:

- View the current site configuration
- Modify or remove a site
- Add or remove teams from a site
- Add or remove Recording Clusters from a site
- Enable or disable automated software updates for client desktops associated with a specific site
- Change the default site
- Specify when, where, and how many uploads can occur

- Schedule uploading of peak and off-peak recordings from the agent desktops to the Site Upload servers

Table 55. Site Settings fields

Field	Description
Default Site	The default site is assigned to new teams that have not been associated with a site. In rare circumstances, it also becomes the default site when a service cannot find a site for a recording.
Site Name	The name of the site.
Enable Automatic Updates for all QM Clients	When selected, enables automated software updates for client desktops associated with the selected site.
Peak Hours Begin	The time, in 24-hour format, when peak hours in the contact center begin. Must be between 00:00 and 23:59 in 1-minute increments. Default = 09:00.
Peak Hours End	The time, in 24-hour format, when peak hours in the contact center end. Must be between 00:00 and 23:59 in 1-minute increments. Default = 17:00.
Max Peak Hour Uploads	The maximum number of recordings that can upload simultaneously during peak hours. Must be a value from 1 to 100. This limit is set to conserve bandwidth on the network. When one upload completes, another takes its place, but there can be no more than the configured number uploading at any one time. Default = 5.
Max Off Hour Uploads	The maximum number of recordings that can upload simultaneously during off hours (the hours not specified as peak hours as defined by the Peak Hours Begin and Peak Hours End fields). Must be a value from 1 to 200. This limit is set to conserve bandwidth on the network. When one upload completes, another takes its place, but there can be no more than the configured number uploading at any one time. Default = 100.
Storage Location	You can change the storage location to any local or external folder. You do not have to store recordings on the machine that hosts the Site Upload Server. NOTE: If you are using remote storage, the File Transfer Servlet that is part of the Site Upload Server must run as a user who has access to the location you choose for recordings.
IP Address	The IP address of the machine that hosts the Site Upload Server and the voice recordings, and the path where voice recordings are stored.

Table 55. Site Settings fields (Continued)

Field	Description
Local Storage Location	Choose this option to store the voice and screen recordings on the Quality Management server.
External Storage Location	<p>Choose this option to store the voice and screen recordings on an external server.</p> <p>NOTE: If you change the storage location from local to external storage in update mode, you must first uninstall the PROXY Pro Gateway service on the server that hosts the Site Upload Server (in the Control Panel's Add or Remove Programs, remove PROXY Pro Gateway). When you run the Set Recording Home Directory tool, the PROXY Pro Gateway service is reinstalled automatically. See "Entering Configuration Data in Update Mode" on page 183 for more information.</p>
Storage Location Path	<p>The path where voice and screen recordings are stored. Click Browse and navigate to the storage folder.</p> <p>NOTE: The default path is C:\Program Files\Common Files\QM\Recordings. If you need to change the path, do not specify the root directory (for example, D:\ or E:\). Always include at least one folder in the path (for example, D:\Cisco).</p>
Username	<p>If you selected an external storage location, enter the username required to access that location. If the user is a domain user, enter the name with the format <domain>\<username>.</p> <p>For external screen storage and playback to work, you must provide a domain user that has read and write access to the local server and the external storage system.</p> <p>This user must meet these requirements:</p> <ul style="list-style-type: none"> • The local server must know the user (the user is a trusted domain user). • If the user is a domain user, the domain specified must be trusted by the local server. This means the Voice Record Server that you are configuring has to be on a domain that trusts or is trusted by the domain you are entering. • The user must be able to log on as a service. • The user must have read and write access to both the external drive location entered AND the location where Quality Management is installed on the local server.
Password	If you selected an external storage location, enter the password required to access that location.
Teams	A list of available teams.

Table 55. Site Settings fields (Continued)

Field	Description
Assigned Teams	A list of teams assigned to this site.
Recording Clusters	A list of available Recording Clusters
Assigned Recording Clusters	A list of Recording Clusters assigned to this site.

Table 56. Site Settings buttons

Field	Description
Delete Selected Site	Remove an existing site.
Browse	Locate a folder.
>	Move selected teams in the teams list to the Assigned Teams list.
>>	Move all teams in the Teams list to the Assigned Teams list.
<	Move selected teams in the Assigned Teams list to the Teams list.
<<	Move all teams in the Assigned Teams list to the Teams list.

Configuration Settings Used By Services

If you change the settings on the Site Settings window, the following table shows when your changes take effect.

Table 57. When services start using the changed configuration settings

Service	Configuration settings applied when...
Upload Controller service	The next End of Day applies the configuration settings. If you want the changes to take effect immediately, restart the Upload Controller service.
DB Cleaner service	The next cleanup time applies the configuration settings. If you want the changes to take effect immediately, restart the DB Cleaner service.

Table 57. When services start using the changed configuration settings (Continued)

Service	Configuration settings applied when...
FTS webapp (Jetty service)	Restart the Jetty service.

Site Considerations

If you plan to use multiple recording storage locations, you can associate each recording storage location to a site.

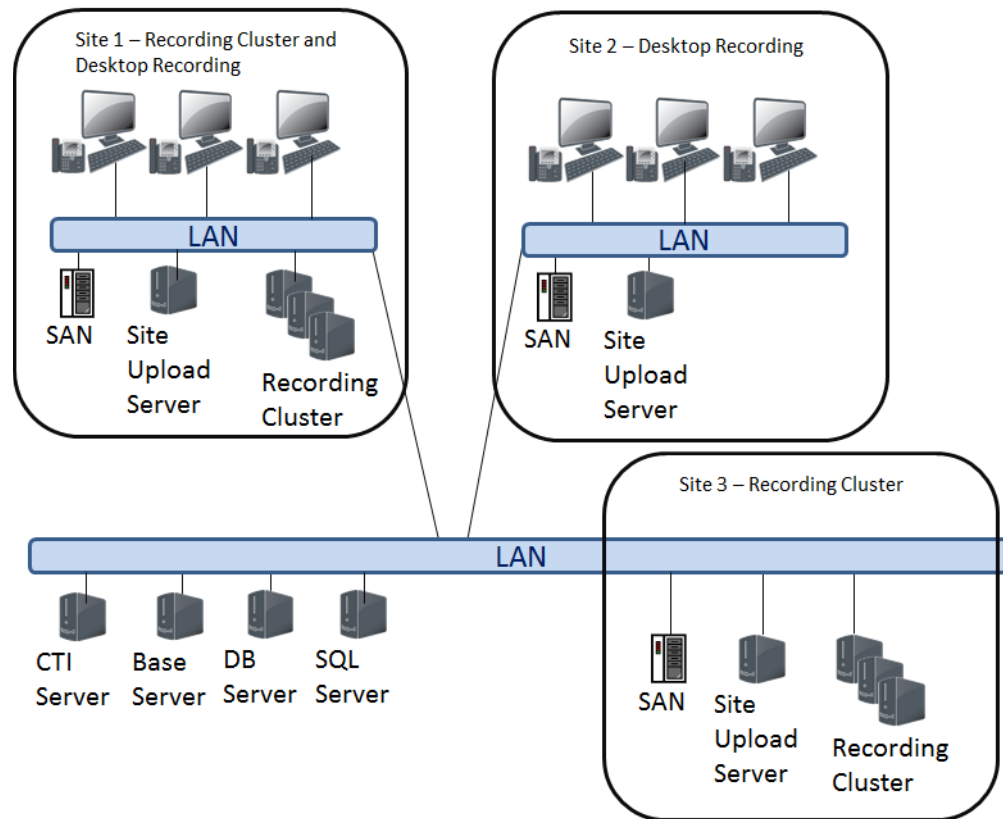
When configuring sites, consider the following:

- A site is a single Site Upload server associated with a set of teams. A site can be configured to be the system’s default site. The default site is used for teams that have not been associated with a site or whenever a recording service cannot find a site for a recording (this can happen in rare circumstances).
- You can configure one or more sites for a Quality Management system and define the teams that are assigned to each site.
- When a site is taken down for maintenance or failure, the recordings created by the agents while the site was down will be uploaded when the site recovers.
- When upgrading from 9.0 or earlier, Quality Management will create a single site and assign the Site Upload server, Upload Controller service, and all defined teams to that site. Peak and off-peak settings will also be moved to the site. Once Quality Management is installed, you can add more sites.
- When an agent plays a recording from the Recordings application, the Recordings application will play back the recording from the Site Upload server that is associated with the agent’s team.
- For Desktop Recording, Quality Management records the agent’s calls while the agent is logged in to the client desktop. When the agent logs out, the recordings are uploaded to the Site Upload server that is associated with the agent’s team. It is possible to have two different agents using the same computer at different times and have their recordings uploaded to different Site Upload servers.

[Figure 27](#) shows three sites—two external sites that communicate with the rest of the system over a WAN and one site that communicate over a LAN. Each site has a Site Upload server with an Upload Controller and a Recording Cluster. Each site has one or more teams assigned to it and the users in those teams will upload to the proper site.

For example, the Base server is located in the United States (site 3) and a Site Upload server is located in Germany (site 1) and all the German teams or groups are assigned to the German site. When a German agent records a call, the recording is uploaded to the German site recording storage location in Germany. When the agent plays back the recording, the recording is retrieved locally and avoids wide area network (WAN) traffic.

Figure 27. Multiple site configuration example



Software Updates

Use the Automated Update feature to update the Quality Management Administrator and Desktop Recording service. When you enable the Automated Update feature, every time a client application starts, it checks the services for Quality Management to determine if a newer version is available. If there is a newer version, the Automated Update feature automatically installs the update on the client desktop.

NOTE: If you apply a Service Release (SR) update to the system, the best practice is to disable the Automated Update feature first. After the SR update is installed, manually test an updated instance of the Desktop Recording service, Workforce Optimization, and Quality Management Administrator to verify they work. When you are satisfied they work, you can re-enable the Automated Update feature.

Use the Automated Update feature to update up to 500 client desktops. If your site has more than 500 client desktops, Cisco recommends using push notifications.

Patches

When you install a patch on the server that includes patches for the client desktop, the patch installs a webpage called Patches.htm on the server. If the automatic update feature is disabled, you can download the patch for the client desktop from <http://<Base server>/TUP/QM/Patches.htm>.

Managing Site Settings

TASK

- To view the existing site configuration, click Site Settings.

STEP RESULT: The Site Settings window appears.

- To view a different site, click the tab associated with the site.

ADDITIONAL INFORMATION: New sites appear in Site settings when you install Quality Management on the server associated with the new site and configure the new site in the Site Settings window.

- To remove a site, click the tab for the site you want to remove, click Delete Selected Site, click Yes in the Confirm Delete dialog box, choose where you want to move recordings from the deleted site, and then click OK.

STEP RESULT: The Manually Move Recordings dialog box appears. You need to manually move the existing recordings from the server associated with the old site to the server associated with the new site. The teams from the old site are now assigned to the new site and future recordings for those teams will now be stored on the server for the new site.

- To modify a site, select the site's tab, complete the fields, and then click Save.
- To change the default site, select a site from the Default Site drop-down list, and then click Save.
- To enable or disable automatic updates on client desktops associated with a site, click the tab for a site, select or clear the Enable Automatic Updates for all QM Clients check box, and then click Save.
- To modify the current upload settings for a site, click the site's tab, complete the fields under Peak Uploads, and then click Save.
- To change the recording storage location, complete the fields under Storage Location and then click Save.
- To add teams or Recording Clusters to a site, select the site's tab, select one or more teams or Recording Clusters from the Teams or Recording Clusters list and click the > button to move the teams to the Assigned Teams or Assigned Recording Clusters list. To move all teams

or Recording Clusters to the Assigned Teams or Assigned Recording Clusters list click the >> button, and then click Save.

- To remove teams or Recording Clusters from a site, select the site's tab, select one or more teams or Recording Clusters from the Assigned Teams or Assigned Recordings Clusters list and click the < button to move the teams to the Teams or Recording Clusters list. To move all teams or Recording Clusters to the Teams or Recording Clusters list click the << button, and then click Save.

Inclusion List

Quality Management uses the Inclusion List window (Figure 28) to determine which calls to record and which calls to ignore. Quality Management only records calls that match the extension patterns in the Patterns to be Recorded list.

Figure 28. Inclusion List window

The screenshot shows the 'Inclusion List' window for 'Telephony Group: group1'. It contains two main sections:

- Patterns to be Recorded:** A table with columns 'Pattern', 'Type', and 'Direction'. One entry is visible: Pattern '*', Type 'Extension', and Direction 'Either'. Below the table are buttons for 'Add', 'Remove', 'Modify Type', and 'Modify Direction'. There are also up and down arrow buttons to the right of the table.
- Patterns to be Excluded from Recording:** A table with columns 'Pattern' and 'Type'. It is currently empty. Below the table are buttons for 'Add', 'Remove', and 'Modify Type'.

A tab appears in the Inclusion List window for each configured telephony group. You can configure extension patterns for inclusion or exclusion for each telephony group.

If you are using Cisco MediaSense Recording, the Inclusion List affects which recordings are uploaded to Quality Management. Initial recording decisions are based on the Cisco MediaSense configuration.

The Patterns to be Recorded list contains extension patterns that will be recorded. By default, the Patterns to be Recorded list displays an asterisk (*) in the Pattern column, Extension in the Type column, and Either in the Direction column. This indicates that all incoming and outgoing calls on all extensions in the telephony group will be recorded. As soon as specific extension patterns are configured in the Patterns to be Recorded list, recording is limited to those extension patterns only.

The Pattern column lists the extension pattern that will be filtered in the Patterns to be Recorded or Patterns to be Excluded from Recording lists. You can use the following wildcards to configure ranges:

- The asterisk (*) in a string can represent any quantity of any character, as long as the other characters in the string match.
- The question mark (?) in a string can be replaced by any character, but the length of the string must be exactly as represented.

Extension patterns can be further filtered by selecting:

- The direction of the call (for recorded calls only). Your options are:
 - Inbound—filters all inbound calls that match the extension pattern
 - Outbound—filters all outbound calls that match the extension pattern
 - Either—filters all inbound and outbound calls that match the extension pattern
- The type of call. Your options are:
 - Any—filters all called, calling, and extensions calls that match the extension pattern
 - Called—filters all calls received by the phone numbers that match the extension pattern
 - Calling—filters all calls made by the phone numbers that match the extension pattern
 - Extension—filters all extensions that match the extension pattern

A scroll bar is available if you add more than 9 extensions to the list. Use the scroll bar to move up and down the list.

To rearrange the order of extension patterns that appear in the Patterns to be Recorded list, select an extension pattern from the list and use the Up or Down arrow buttons to move the extension pattern to the desired location. Extension patterns are filtered starting at the top of the list and continues down to the bottom of the list.

The Patterns to be Excluded from Recording list displays extension patterns that will not be recorded. Extension patterns that appear in the Patterns to be Excluded from Recording list are filtered before any extension patterns that appear in the Patterns to be Recorded list. Only extension patterns found in the Patterns to be Recorded list will be recorded.

Any changes you make to the Inclusion List take window take effect at the next recording client login.

Table 58. Inclusion List buttons

Field	Description
Add	Add an extension pattern.
Remove	Remove an extension pattern.
Modify Type	Change the call type associated with an extension pattern.
Modify Direction	Change the direction associated with an extension pattern.

Managing Extension Patterns

Use this task to add a extension pattern to the Inclusion List.

TASK

1. Select the appropriate telephony group cluster tab in the Inclusion List window.
2. Choose one of the following options:
 - Add an extension pattern. Click Add beneath the Patterns to be Recorded or Extensions to be Excluded, type a number in the Add Pattern dialog box, click OK, and then complete the remaining fields in the table.

You can enter the exact number or use the * or ? wildcards plus numbers to configure a range of numbers. For example:

Enter This:	To Record:
6124	Number 6124.
61*	Any number that start with 61 and are of any length (for example, 6124, 61555, 613).

Enter This:	To Record:
61??	Any number that start with 61 and are 4 digits long (for example, 6124, 6125, 6126).

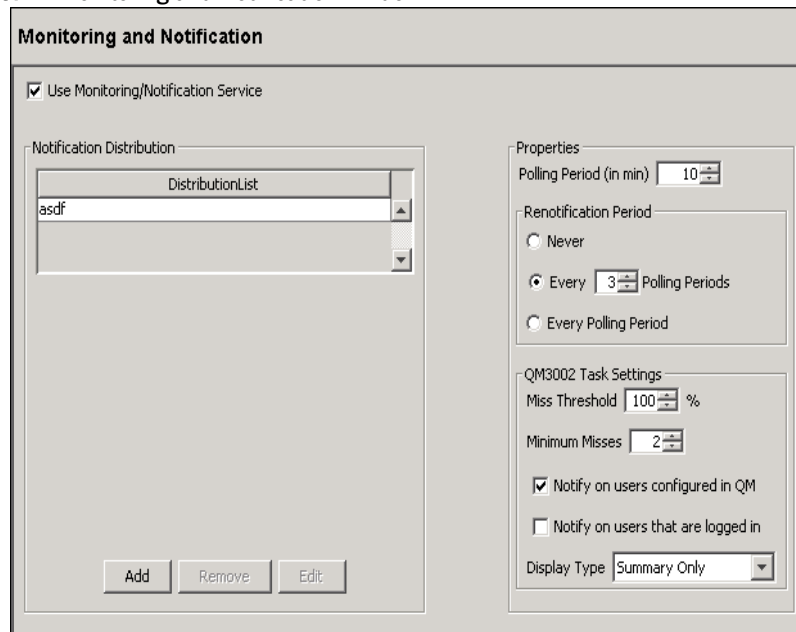
- Modify a call type. Select an extension pattern, click Modify Type, select the different type from the drop-down list, and then click OK.
- Modify a call direction. Select an extension pattern, click Modify Direction, select a different direction from the drop-down list, and then click OK.
- Remove an extension pattern. Select the extension pattern in Patterns to be Recorded or Extensions to be Excluded, click Remove, and then click OK.

3. Click Save.

Monitoring and Notification

Use the Monitoring and Notification window (Figure 29) to enable the Monitoring and Notification (MANA) service.

Figure 29. Monitoring and Notification window



Only one notification trigger requires configuration: Problem ID QM3002 under QM Task Settings. This trigger compares data in the Unified CM's Call Detailed Records (CDR) Report (for Unified CM version 9.x) with the Quality Management database.

Specifically, it compares the call records in the Unified CM with the call records in Quality Management. If there is a discrepancy, notification is sent.

NOTE: The MANA CDR Report (QM3002 notification trigger) does not support devices that are recorded by Cisco MediaSense. If your site is a mixed-recording environment where Server Recording, Network Recording, or Desktop Recording and Cisco MediaSense Recording are used together, the CDR Report will not be accurate since Cisco MediaSense devices result in false positives.

By default, Problem ID QM3002 is disabled. The notification trigger does not have to be configured unless you enable that problem ID in the Notification Distribution dialog box.

You can create multiple distribution lists. For each distribution list, you can choose to specify the events that trigger notification. For example, you can set up a distribution list for global outages (all QM1000 level errors) and all “JTAPI not associated with a device” (specific QM2002 error).

You can also configure the following information.

- Distribution list of persons receiving notification, if you configure email as a means of notification
- Email address of the person(s) receiving notification, if you configure email as the means of notification
- Trap destinations receiving notification, if you configure SNMP as the means of notification
- If and how often a renotification of the problem should be sent out
- Types of problems that will trigger notification

NOTE: You can only change the information in the Monitoring and Notification window from the System Configuration Setup (PostInstall.exe) or Quality Management Administrator on the Base server. The Monitoring and Notification window in Quality Management Administrator on a client desktop is read-only.

Connection information is saved locally to the Base server so the emergency user can still be notified using email if a major component (for example, the database) is down, and the other email addresses are not available. This allows the Quality Management administrator to edit the emails and allows Monitoring and Notification to notify one user when the configuration is not accessible.

Table 59. Monitoring and Notification fields

Field	Description
Use Monitoring/ Notification Service	Select this check box to enable the MANA service. If enabled, at least one notification method (event viewer, SNMP, or email) must be enabled as well. This check box is selected by default.
Distribution List	The available distribution lists.
Polling Period	Sets the interval at which the MANA service checks for the selected notification triggers. Default = 10 minutes, Minimum = 0 minutes, Maximum = 1440 minutes (1 day). The timer starts when the last polling task is complete. NOTE: When you change the polling period, it takes one polling cycle before the new polling period goes into effect.
Never	Choose this option if you do not want to be renotified of a problem after the initial notification.
Every N Polling Periods	Choose this option if you want to specify how frequently you want renotification to occur after the initial notification and specify the number of polling periods. For example, if you choose to be notified every 3 polling periods, you receive the initial notification on the first polling period the problem is detected, no notification the next two polling periods, and then another notification on the next polling period. This pattern will continue as long as the problem is detected.
Every Polling Period	Choose this option if you want renotification to occur every polling period after the initial notification.
QM3002 Task Settings	The fields listed in the QM Task Settings section are used to configure QM3002.
Miss Threshold	Percentage of missed CDRs required to trigger notification.
Minimum Misses	Lowest number of missed CDRs required to trigger notification.
Notify on users configured in QM	When you select this option, Quality Management only generates notifications about users who are configured in Quality Management Administrator.
Notify on users that are logged in	When you select this option, Quality Management only generates notifications about users who are currently logged in to Workforce Optimization. This only applies to the Desktop Recording service.

Table 59. Monitoring and Notification fields (Continued)

Field	Description
Display Type	<p>Choose one of the following options.</p> <ul style="list-style-type: none"> Summary Only—displays 1 row per agent with missed CDR that meet the above criteria Details (Tab Delimited)—displays each missed CDR in tab delimited format Details (Plain Text)—displays each missed CDR in text format

Table 60. Monitoring and Notification buttons

Field	Description
Add	Add an email address.
Remove	Remove an email address.
Edit	Edit the selected email address.

Configuration Settings Used By Services

If you change the settings on the Monitoring and Notification window, the following table shows when your changes take effect.

Table 61. When services start using the changed configuration settings

Service	Configuration settings applied when...
MANA service	The next polling period applies the configuration settings.

Configuring the QM3002 Notification Trigger

This task describes how to configure the QM3002 notification trigger.

TASK

1. Click CDR Configuration in the Monitoring and Notification window.

STEP RESULT: The CDR Configuration dialog box appears.

2. Select the version of the Cisco Unified CM you are using from the drop-down list.

3. Choose Host Name or IP Address, and then enter the information for the Unified CM.
4. Type the Unified CM username and password.

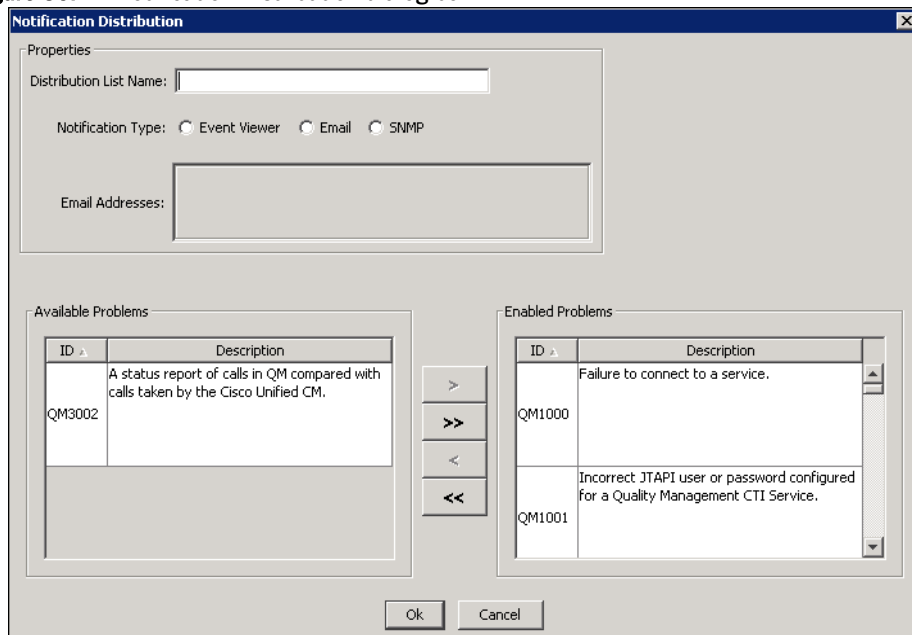
ADDITIONAL INFORMATION: Enter the name and password of the user with rights to access the CAR reports.

5. Add the extensions that you do not want to receive notifications.
6. Configure the properties for the notification.
7. Click OK.

Notification Distribution

The Notification Distribution dialog box (Figure 30) allows you to create a distribution list, specify the notification type for the distribution list, and assign the type of MANA messages that are sent to the distributions list.

Figure 30. Notification Distribution dialog box



The MANA messages are classified as follows:

- QM1xxx—indicates a global outage that might affect recording for the entire system.
- QM2xxx—indicates individual outages that might affect recording for individual users.

- QM3xxx—indicates a possible configuration problem. The notifications might not point to an actual issue, so you might want to turn these notifications off to avoid unnecessary notifications.
- QM4xxx—indicates a problem with MANA that prevents it from reporting problems.

Table 62. Notification Distribution fields

Field	Description
Distribution List Name	The name of the distribution list.
Notification Type	The type of notification you want to use to send notification messages. Your options are: <ul style="list-style-type: none"> • Event Viewer—use the Event Viewer for displaying notification messages • Email—use email for sending notification messages • SNMP—use SNMP for sending notification messages
Email Addresses	The list of email addresses to which notification is sent. Maximum = 5 email addresses. NOTE: This field is enabled when you select Email as your notification type.
Available Problems	The list of problems that will not trigger notification. Move any problem that does not require notification to the Available Problems list. By default only QM3002 appears in this list.
Enabled Problems	The list of problems that will trigger notification. By default, all problems except for QM3002 are enabled. You must configure QM3002 under QM Task Settings in the Monitoring and Notification window before enable this Call Detail Record (CDR) task. NOTE: QM3002 is not supported with MediaSense Recording. See “Configuring the QM3002 Notification Trigger” on page 177 for more information.

Managing Notification Distribution Lists

Use this task to manage notification email addresses.

TASK

- To add a distribution list, perform the following steps.
 - a. Click Add in the Notification Distribution section.
 - b. Type the name of the distribution list in the Distribution List Name field.

- c. Type the email addresses that are included in the distribution list in the Email Addresses field.
- d. Move the type of problems you want sent to this distribution list to the Enabled Problems list.
- e. Click OK.

STEP RESULT: The new distribution list appears in the Distribution List.

- To remove a notification distribution list, select the distribution list from the Distribution List, click Remove, and then click OK.

STEP RESULT: The distribution list is removed from the Distribution List.

- To edit a notification distribution list, select the distribution list from the Distribution List, and click Edit. In the Notification Distribution dialog box, modify the distribution list that you want to change, and then click OK.

Enabling or Disabling a Notification Trigger

PREREQUISITE

When enabling the QM3002 notification trigger:

- CDR must be correctly configured in the Unified CM Administration web application. In these versions, there is no CDR database. Instead, the CAR reports (CDR export) are used. Set up CAR so that it updates its information as frequently as possible (less than 30-minute intervals). Create a CAR user and enter that user in the Quality Management CDR Configuration dialog.
- Archiving must be enabled in Quality Management.

This task describes how to enable and disable a notification trigger from the Notification Distribution dialog box.

TASK

- To enable a task notification trigger, choose a trigger from the Available Problems section and click >. The trigger moves to the Enabled Problems section.
- To enable all task notification triggers, click >>. All triggers move to the Enabled Problems section.

- To disable a task notification trigger, choose a trigger from the Enabled Problems section and click <. The trigger moves to the Available Problems section.
- To disable all task notification triggers, click <<. All triggers move to the Available problems section.

Examples of Notification Configuration Problems

The following setup examples illustrate what happens when you configure the Notification Trigger Configuration as described.

Setup 1	<p>Miss Threshold: 50%</p> <p>Minimum Misses: 5</p> <p>Notify on users configured in QM: Enabled</p> <p>Notify on users logged in: Enabled</p>	
Agent		<p>Agent A has 8 matched calls and 2 missed calls. Agent A is properly configured and was logged in for the whole time.</p> <p>Agent B has 6 matched calls, but 2 were made before he was logged in. Agent B is configured properly.</p> <p>Agent C has 2 matched calls and 8 missed calls. Agent C is properly configured and was logged in the whole time.</p>
Effect		<p>Agent A: The missed percentage is $2/(8 + 2) = 20\%$. No notification would be made because neither the Miss Threshold nor the Minimum Misses criteria were met.</p> <p>Agent B: No notification would be made because the Minimum Misses criterion (5) was not met.</p> <p>Agent C: The missed percentage is $8/(2 + 8) = 80\%$. Notification is made because the Miss Threshold and the Minimum Misses criteria were met.</p>

Setup 2	Miss Threshold: 100% Minimum Misses: 1 Notify on users configured in QM: Enabled Notify on users logged in: Disabled.	
Agent		Agent A is configured in Quality Management but does not have the Desktop Recording service installed or the phone is not daisy-chained properly.
Effect		Notification will be made on Agent A's extension, with the agent listed as "Unknown" because there is no cross-reference between the agent and extension until the Desktop Recording service is configured.

NOTE: Matching the CDR or CAR Report with Quality Management is not 100% accurate. CDR data can be out of sync with Quality Management, or certain call scenarios might yield false positives. It should not be used for compliance.

NOTE: Agent team association and whether a team is configured for archiving are determined from the time the CDR task is run, not from the time of the call in question. This could result in either false positives or false negatives if a team's archiving status changes, or if an agent's team membership changes during the period the CDR task is examining.

When a notification is received, look at the DNs/Agents that show missed calls. A large number of agents with missed calls might indicate a Quality Management service failure. The possible services with issues are:

- Load-balancing subscription service
- Upload Controller
- DB Proxy service (on the Database server)

A 100% miss percentage for a single agent might indicate a failure in the Desktop Recording service. If notifications are occurring frequently with less than 100% missed for a small number of agents, the thresholds might need to be adjusted to minimize unnecessary notifications. Even a high threshold (100%) will notify on moderate and major outages.

Status

The Status window reports the version of the installed Quality Management components.

Configuration Settings Used By Services

If you change the product version, the following table shows when your changes take effect.

Table 63. When services start using the changed configuration settings

Service	Configuration settings applied when...
Upload Controller service	Periodically check for a version mismatch.

Entering Configuration Data in Update Mode

There are two ways to change System Configuration Setup data after it is initially entered.

- Change the information through the System Configuration node in Quality Management Administrator.
- Start System Configuration Setup from the executable PostInstall.exe, located on each server in C:\Program Files\Cisco\WFO_QM\bin.

When System Configuration Setup starts, it runs in Update Mode.

Rules for Upgrading or Modifying the Unified CC Database in Update Mode

Observe the following rules when you change access to the Unified CCX database in update mode:

- Do not change the location of the Unified CCX database after initial setup. If you do, you might be unable to access Quality Management historical data if the structure and contents of the new database is not the same as that of the old database.
- Stop the Sync Service and disable this service on startup to protect the Quality Management database before you upgrade or rebuild the Unified CCX database.

Stopping the Sync Service Before Upgrading the Unified CCX Database

Use this task to stop the Sync Service before you upgrade the Unified CCX database.

TASK

1. Select Start > Administrative Tools > Services.

STEP RESULT: The Services window appears.

2. Right-click Monitoring and Recording Sync Service and choose Stop.
3. Right-click Monitoring and Recording Sync Service again and choose Properties.

STEP RESULT: The Monitoring and Recording Sync Service Properties window appears.

4. Choose Disabled from the Startup Type drop-down list, and click OK to save your changes.
5. Upgrade or rebuild the Unified CCX database.
6. Return to the Services window, right-click Monitoring and Recording Sync Service and choose Start.
7. Right-click Monitoring and Recording Sync Service again, choose Automatic from the Startup Type drop-down list, and then click OK to save your changes.

STEP RESULT: This action enables the Sync Service on startup.

NOTE: Do not start Sync Service and enable the Sync Service for the hardware profile until both Unified CCX Administration databases (if using High Availability) are running and synchronized because the Sync Service reads data from the Unified CCX database. Failing to do so could potentially deactivate users if there is a problem with the Unified CCX upgrade or rebuild.

8. Verify the teams and agents in the upgraded Unified CCX appear correctly.

Changing the Base Server

TASK

1. From the System Configuration Setup tool, choose File > Choose Base Server.

STEP RESULT: The System Configuration Setup dialog box appears window appears.

2. Choose the network address type. Your options are:
 - IP Address—the IP address of the Base server.
 - Host Name—the FQDN or hostname of the Base server.
3. Enter the IP address or hostname of Base server.

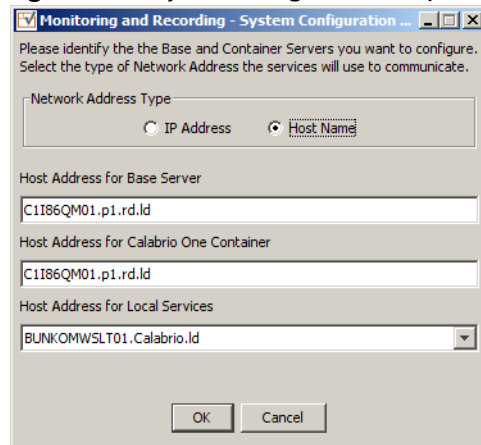
ADDITIONAL INFORMATION: The Base server is the computer where you installed the Base Services, Database Services, Voice/Screen Services, and Load-balancing Subscription service.

4. Enter the IP address or hostname of the Workforce Optimization Container.

ADDITIONAL INFORMATION: The Workforce Optimization Container is located on the Base server.

If you also purchased Workforce Management (WFM) and/or Calabrio Speech Analytics, these products will share this container once they are configured to point to this container. [Figure 31](#) displays the System Configuration Setup dialog box.

Figure 31. System Configuration Setup dialog box



5. Choose one of the following options:
 - If you are running System Configuration Setup on the Base server, choose the IP address or hostname of the Base server from the Local Services drop-down list, and then click OK.
 - If you are running System Configuration Setup on a different server, choose the IP address or hostname for the server from the Local Services drop-down list, and then click OK.

ADDITIONAL INFORMATION: For example, if you want to run Network Recording on a different server and installed the Network Recording service and Monitor service

on that server, choose the IP address for the Network Recording server from the IP Address for Local Services drop-down list. If the computer has multiple NICs, multiple addresses appear in the IP Address for Local Services drop-down list. Choose the IP address used for network traffic.

Changing Quality Management Configuration Data in Update Mode

Use this task to change the configuration data in update mode.

TASK

1. Start System Configuration Setup by running the PostInstall.exe.

ADDITIONAL INFORMATION: This executable is located in the C:\Program Files\Cisco\WFO_QM\bin folder.

2. Select the window you want to modify from the left pane, enter the new data in the right pane, and then click Save on the toolbar or File > Save from the menu bar.
 - You can display the windows in any order you wish.
 - If you modify something in a window, you must click Save to save your changes before you move on to another window.
 - If you make a change to a window but need to change back to the original setting, click the Revert to Saved button on the toolbar. This discards any changes you made that have not been saved, and restores the settings in the window to the last saved version.
3. When you finish, choose File > Exit or click Close.

STEP RESULT: System Configuration Setup closes.

4. Stop and restart the modified service and all desktops for the change to go into effect.

System Configuration Setup Tools

System Configuration Setup provides a number of tools you can use to update your site information. These tools are available through the Tools menu. These tools normally run during the initial installation of Quality Management.

The Tools menu, in System Configuration Setup, only enables tools when the tools are available on the server where you are running the System Configuration Setup tool.

Table 64 displays the available tools and the servers on which they are located.

Table 64. Tool availability in the System Configuration Setup tool

Tool	Base Server	Database Server	Site Upload Server	CTI Server	Record & Monitor Server
Start Local Services	x	x	x	x	x
Create Database Catalogs	x	x			
Generate Info for MSI Clients	x				
Download/Install JTAPI				x	
Encrypt Audio Files			x		
Set Recording Home Directory			x		
Show Proxy Networks Administrator	x				
Generate SSL Certificates	x		x		
Test CTI Service(s)	x	x	x	x	x
Test MediaSense Subscription Service	x	x	x	x	x
Display Metadata Encryption Key	x	x	x	x	x
Choose Monitor Adaptor					x
Remove Recording Services	x	x	x	x	x
Set Temporary Recording Directory					x
SIP Trunk Certificate					x

Start Local Services

This tool offers a convenient way to start all the Quality Management that are on the local computer. You can run this tool any time. However, you should notify users because restarting services might cause outages.

Create Database Catalogs

This tool creates a new Quality Management database if one does not exist or updates an existing database to the latest schema version without overwriting any existing data. You can use this tool to recreate your Quality Management database if you have no backup database and your database was corrupt and you deleted it. This tool populates a fresh database when the Unified CCX and Data API sync with it.

Generate Info for MSI Clients

This tool updates the information required by the MSI client installation programs to successfully install Calabrio Screen Player Plug-in, the Desktop Recording service, Recording Thin Client, and Quality Management Administrator.

Download/Install JTAPI

Use this tool when you upgrade Unified CM. This tool downloads and installs JTAPI.

Encrypt Audio Files

This tool enables you to encrypt any unencrypted audio files. Run this tool only after you upgrade all client desktops to the latest version of Quality Management. All audio files are encrypted after you run this tool.

Set Recording Home Directory

This tool allows you to restart services after you update the Site Settings window. Run this tool when upgrading from the Basic license to the Advanced license.

Show Proxy Network Administrator

This tool displays the Gateway Administrator. Use this tool when you need to modify the Screen Playback Gateway information.

Generate SSL Certificate

This tool generates a security certificate for the File Transfer Servlet (FTS) and Workforce Optimization-generated reports. Use this tool if your certificate is corrupt or if the IP address of the server changes (the user sees a Security Alert dialog box whenever the FTS or Reports runs). This tool is available only when you run System Configuration Setup on the Quality Management server (for reporting) and the Site Upload server (for FTS).

When you run the tool, you see a Security Alert dialog box. Click View Certificate to display the Certificate dialog box, and then Install Certificate to install a new certificate.

Test CTI Services

This tool verifies that the local Recording CTI service has the correct JTAPI and accepts connections. The tool makes a request to each running Recording CTI service and, if all succeed, returns a success message. If any requests fail, Quality Management reports the failure and lists which succeed. The reports are available in Workforce Optimization.

NOTE: This tool is not required for MediaSense Recording.

If you made any changes to the Recording CTI service in System Configuration Setup, you must restart the Recording CTI service before you run this test.

Test MediaSense Subscription Service

This tool verifies that the running MediaSense Subscription Service has the correct connection and authentication information and accepts connections. This tool makes a request to the MediaSense Subscription Service and, if it succeeds, it returns a success message. If the request fails, Quality Management reports the failure.

If you made any changes to the MediaSense Subscription Service in System Configuration Setup, you must restart the Monitoring and Recording Services MediaSense Subscription service before you run this test.

Display Metadata Encryption Key

This tool displays the customer-specific key used for Advanced Encryption Standard (AES) encryption. This key can be used by external applications to access encrypted user-defined metadata directly from the Quality Management database. You must provide the administrator's user name and password to access this information.

Choose Monitor Adaptor

This tool displays a dialog that asks for the IP address of the NIC card used for the Monitor service and server-based monitoring. This might be different from the network IP address you entered during System Configuration Setup.

The monitor adapter dialog pops up automatically during System Configuration Setup if multiple NIC cards are on the box and the box hosts the Monitor service. You should choose the IP address of the NIC card that you connected to the SPAN port on the switch.

NOTE: This tool is not required for MediaSense Recording.

Remove Recording Services

Use this tool to finalize the removal of Network Recording service and Monitor service servers by removing them from database. Uninstall the services from the server before you use this tool.

Set Temporary Recording Directory

This tool allows you to choose a temporary storage location for recordings before they are uploaded. You can change the temporary storage location at any time. When you change the temporary storage location, System Configuration Setup moves the recordings to the new location.

SIP Trunk Certificate

Use this tool to generate, upload, or download a SIP trunk certificate. A SIP trunk certificate is required when your system is configured for Network Recording with Cisco Unified CM 8.0 or later.

NOTE: This tool is not required for MediaSense Recording.

Generate SIP Trunk Certificate

Use this tool to generate a SIP trunk certificate. The SIP trunk certificate is saved to the C:\Program Files\Common Files\QM\Certificates folder.

Upload SIP Trunk Certificate

Use this tool to upload a SIP trunk certificate from a flash drive or folder.

Download SIP Trunk Certificate

Use this tool to download the SIP trunk certificate to a flash drive or folder. Follow the upload instructions in the Cisco Unified Communications Manager Administration Guide to upload the certificate to Cisco Unified CM.

If you are using multiple Voice Record Servers, copy the Certificates directory containing both privacy-enhanced mail (PEM) files to the same location on the other Voice Record Servers.

External Storage and Services

If you select External Storage Location in the Site Settings window in System Configuration Setup, you must configure the Jetty service and the Screen Playback Gateway (PROXY Pro Gateway) service.

This step must be done after you install the Monitoring and Recording Services Base Services and before you start recording contacts.

To use external storage, you perform the following procedures.

1. Create a username and password for the external storage user on the external storage server.
2. Configure the Jetty service and PROXY Pro Gateway service for external storage.

Configuring Services for External Storage

TASK

1. Select Start > Administrative Tools > Services.

STEP RESULT: The Services window appears.

2. Right-click Monitoring and Recording Jetty service and choose Properties.

STEP RESULT: The Monitoring and Recording Jetty Service Properties window appears.

3. Click the Log On tab, choose This Account, complete the fields, and then click Apply.

ADDITIONAL INFORMATION: Provide the username and password for the external storage server.

STEP RESULT: If the provided information is correct, the following message will appear:

```
The account .\<username> has been granted the Log On As A  
Service right.
```

where `<username>` is the username you provided in the This Account field.

4. Repeat [step 2](#) and [step 3](#) for the PROXY Pro Gateway service.

Installing Server Applications

You can install the Recording Thin Client from a web page that resides on the Quality Management server. Quality Management creates this web page when you install the Base Services.

The web page is ScreenRecordingThinClient.htm. This page contains a link to the Recording Thin Client. The Recording Thin Client allows screen recording on a Citrix server. The Recording Thin Client does not support the Automated Update feature.

Install the Recording Thin Client on the Citrix server after you install the services for Quality Management.

Installing the Recording Thin Client on a Citrix Server

Use this task to manually install the Recording Thin Client on a Citrix server.

TASK

1. Open the Citrix server's web browser and access the ScreenRecordingThinClient.htm on the Base server.

`http://<Base server>/TUP/QM/ScreenRecordingThinClient.htm`

ADDITIONAL INFORMATION: Where <Base server> is the IP address or hostname for the Base server. Note that this address is case sensitive.

2. Follow the installation instructions on the web page to upgrade the applications on the client desktop.
3. Restart the Citrix server when prompted to ensure the services start correctly.

Configuring the Audio Player for Citrix

By default, Quality Management uses the QmAudioPlayer class. Citrix requires the QmWmpAudioPlayer class.

Configuring the Audio Player Type for Citrix

TASK

1. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.
2. Expand the database name (SQMDB) under the Databases node.
3. Right-click dbo.DbProperties and click Open Table.
4. Change the setting for isCitrix to true.
5. Choose File > Exit to close SQL Server Management Studio.

After Installing Quality Management

Read this section and ensure all tasks are complete after you install Quality Management

CAD Integration

If your environment includes CAD, you can integrate CAD with Quality Management. See the *CAD Integration Guide* for instructions.

Installing Client Applications

Quality Management allows you to use the following options to install the client applications on client desktops.

- Manually install Quality Management client applications on each client desktop.
- Use automated package distribution tools to deploy client applications for Quality Management to the client desktops.

Enabling the Elevated Privileges Policy for Windows Installer Installation

To allow users with limited privileges to install a client application for Quality Management on a computer you must enable the Windows policy “Always Install with Elevated Privileges” for both the User Configuration and the Computer Configuration.

By default, Windows Installer installations run in the context of the logged-on user. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the install to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

Enabling the Windows Elevated Privileges Policy

Use this task to elevate the privileges on a user’s computer so the user can install the client applications for Quality Management.

TASK

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the appropriate organizational unit (OU) and from select Properties from the popup menu.
3. On the Group Policy tab, select the Group Policy Object (GPO) and then click Edit.
4. Expand Computer Configuration > Administrative Templates > Windows Components > Windows Installer.
5. Double-click Always install with elevated privileges.
6. Set to Enabled, and then click OK.

7. Expand User Configuration > Administrative Templates > Windows Components > Windows Installer.
8. Double-click Always install with elevated privileges.
9. Set to Enabled, and then click OK.

ADDITIONAL INFORMATION: You must enable this GPO under both the User Configuration and Computer Configuration sections for it to take effect.

Using Automated Package Distribution Tools

MSI-based desktop application installations for Quality Management can be deployed (pushed) via automated package distribution tools that make use of the Microsoft Windows Installer service.

Requirements

Quality Management support for automated package distribution depends on compliance with the requirements listed below.

Execution

Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.

Per-Machine vs. Per-User

Installations must be deployed on a per-machine basis. Per-user installations are not supported.

Automated Package Installation vs. Manual Installation

Automated installations must use the same files and meet the same installation criteria as manually-deployed installations.

MSI packages for Quality Management are located in the following location on a successfully-installed production server and are intended for both manual and automated deployment.

<user-defined path>\WFO_QM\Jetty\webapps\TUP\QM

You can also generate MSI packages for Quality Management using the ConfigureMsi.exe utility and unconfigured installation templates. See [“Client Installation Packages” on page 199](#) for more information.

Quality Management does not support alteration of these files or the use of other MSI files included with the product at other locations.

The requirements for supported operating systems, product deployment configurations, installation order, and server/client version synchronization for automated package installation is the same as manual installation. Quality Management does not support altering the supplied MSI packages to circumvent the installation criteria.

Multiple Software Releases

Do not combine multiple software releases into a single deployment package. You must distribute each Quality Management software release in its entirety as a distinct deployment. Quality Management does not support combining multiple releases (for example, a software package's base release and a subsequent engineering test) into a single deployment package.

Recommended Deployment Preparation Model

Use the following deployment preparation model to test the deployment in a test environment before you deploy an update on your production server.

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment.

This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in ["Requirements" on page 198](#).
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

Client Installation Packages

The Quality Management installation DVD contains unconfigured installation templates that, with the use of a configuration tool (ConfigureMsi.exe), can be configured so that client applications are available prior to the installation of the services for Quality Management.

The unconfigured installation templates are located in the following file structure on the installation DVD:

- Clients
 - Admin
 - MediaPlayer
 - Recording
 - RecordingThinClient

Configuring Client Installation Files

Use this task to configure client installation files with the ConfigureMsi tool.

TASK

1. Copy the Clients folder and all its contents from the Quality Management installation DVD to a PC that does not have the Quality Management Base Services installed on it.
2. On the desktop, open a command window and navigate to the Clients folder.
3. Type ConfigureMsi.exe and press Enter.

STEP RESULT: The configuration tool starts.

4. Type the IP address or hostname of the Base Host or Surrogate Host and press Enter.
5. Type the IP address hostname of Surrogate Host 1 and press Enter.
6. Type the IP address or hostname of Surrogate Host 2 or `none`, if Surrogate Host 2 does not exist, and press Enter.

STEP RESULT: The utility creates installation files for all Quality Management client applications.

Installing Client Applications for Quality Management

You can install the client applications from web pages that reside on the Quality Management server. Quality Management creates these web pages when you install the Base Services.

Install the client applications after you install the services for Quality Management.

Enabling the Next Generation Java Plug-in

Use this procedure to enable the Generation Java Plug-in so that you can play screen recordings in Workforce Optimization.

TASK

1. From the client desktop, choose Start > Control Panel.

STEP RESULT: The Control Panel window appears.

2. Double-click Java Control Panel.

STEP RESULT: The Java Control Panel window appears.

3. Click the Advanced tab and scroll to Java Plug-in.
4. Select the Enable the next-generation Java Plug-in.
5. Click OK.
6. Restart your web browser.

ADDITIONAL INFORMATION: If you have more than one web browser open, you must restart all web browsers.

Installing Client Applications for Quality Management

Use this task to install client applications for Quality Management.

TASK

1. From the computer where you want to install the desktop application, start Microsoft Internet Explorer.
2. Enter the appropriate installation web page address in the Address field:
 - <http://<Base server>/TUP/QM/Administrator.htm>—This page contains links to the install files for all desktop applications—Quality Management Administrator, Desktop Recording service, and Calabrio Screen Player Plug-in.

NOTE: Quality Management automatically installs Quality Management Administrator on the Base server.

- <http://<Base server>/TUP/QM/Desktop.htm>—This page contains a link to the Calabrio Screen Player Plug-in install files.
- <http://<Base server>/TUP/QM/Recording.htm>—This page contains a link to the Desktop Recording service install files.

STEP RESULT: The installation web page appears.

3. Follow the instructions on the web page to install the desktop application.

ADDITIONAL INFORMATION: If you are running Windows 7, a Reboot Warning dialog box might appear behind the current window after you install the application. Move the current window out of the way to check for the Reboot Warning dialog box.

If you are prompted to reboot the machine to complete the installation, click No. This reboot prematurely terminates background installation activities.

4. Manually reboot the computer before you run Quality Management to ensure your screens are recorded.
5. If available, download the latest SR for the client desktop from <http://<Base server>/TUP/QM/Patches.htm> and follow the instructions on the web page to install the SR.

Removing Quality Management 8.x(x) or later

Uninstall Quality Management in the following order:

1. From the Base server:
 - a. Clear the Enable Automatic Updates for All QM Clients check box on the Site Settings window in Quality Management Administrator.
 - b. Remove Quality Management ETs, if any.
 - c. Remove Quality Management SRs and ESes, if any.
2. From the client desktops, use Programs and Features or Add/Remove to remove the following client applications:
 - Cisco Unified WFO Monitoring and Recording Recording (Desktop Recording service)
 - Calabrio Screen Player Plug-in

NOTE: If you are removing version 8.x(x) before upgrading your software, you can skip this step.

3. From the Base server, use Programs and Features or Add/Remove to remove Cisco Unified WFO Quality Management.

NOTE: If you are prompted to reboot the machine to complete the installation, click No. This reboot prematurely terminates background removal activities. You can manually reboot the machine later.

4. Remove Cisco Unified Communications Manager JTAPI client.
5. Remove PROXY Pro Gateway service.
6. If you were prompted to reboot the machine, reboot the machine now.
7. Some files might not be deleted after you perform these tasks. If the Calabrio folder exists on the machine, delete it. The default path to the Calabrio folder is as follows:

C:\Program Files\Cisco

NOTE: You might not be able to delete the files in the folder because they are locked. To unlock the files, reboot the machine and try again.

Recordings are not uploaded from client or server computers when you remove Quality Management. They are maintained in the folder located at ..\Program Files\Common Files\SQM\Recordings on the same drive where you installed the services for Quality Management.

The default location on the storage server for uploaded recordings is:

C:\Program Files\Common Files\QM\Recordings

If you did not use the default location, you specify the custom location you used when you installed Quality Management.

NOTE: A user must log in as an administrator in order to remove any Quality Management applications.

Removing a Quality Management Application

Use this procedure to uninstall the components identified in [“Removing Quality Management 8.x\(x\) or later” on page 203](#).

TASK

1. Open the Windows Control Panel.
2. Double-click Add or Remove Programs.
3. From the list, select the application you wish to remove and click Remove.

ADDITIONAL INFORMATION: If you are running Windows 7, a Reboot Warning dialog box might appear behind the current window after you install the application. Move the current window out of the way to check for the Reboot Warning dialog box.

If you are prompted to reboot the machine to remove the software, click No. This reboot prematurely terminates background installation activities. You can manually reboot the machine before you install any software.

IMPORTANT: If you have multiple client applications for Quality Management installed on one computer, and wish to uninstall one application and leave the rest, you must uninstall all of the applications, reboot your computer, and then reinstall the desired set of applications. The applications share certain third-party files, and uninstalling one application may remove files needed by the remaining applications.

If you intend to reinstall Quality Management after completely removing an older version (a clean install), verify that the recording storage folder structures are removed before installing the new version.

STEP RESULT: Windows removes the application.

Removing the Quality Management Databases

Using the Windows Control Panel on the Quality Management server to remove services does not remove the Quality Management database (SQMDB).

IMPORTANT: If you intend to reinstall or upgrade Quality Management, and you want to retain historical data, you must not remove the Quality Management database.

To remove the Quality Management database completely, complete the following task.

TASK

1. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.
2. In the left navigation pane, expand the Databases node and right-click SQMDB.
3. From the popup menu, choose Delete.

STEP RESULT: The Delete Object window appears.

4. Select the Close existing connections check box and then click OK.

Backup and Restore

There are two situations when you need to create a backup of Quality Management data.

- Upgrading your system to the latest version of Quality Management.
- Making a disaster recovery backup for Quality Management data.

Quality Management Database Disaster Recovery

Use the Backup and Restore features available in the Microsoft SQL Server Management Studio to back up and restore Quality Management version databases.

The SQMDB database stores historical data and report data.

Back up the databases to a folder on the computer that hosts the Microsoft SQL Server.

NOTE: After you back up the Quality Management database, it is advisable to copy the backup files to another location for safekeeping.

Backing Up the Quality Management Databases

Use this task to back up your Quality Management system.

TASK

1. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.
2. Right-click the database name (SQMDB) under the Databases node.

STEP RESULT: A menu appears.

3. Choose Tasks > Back Up.

STEP RESULT: The Restore Database window appears.

4. Complete the fields and click OK.

Restoring the Quality Management Database

Use this task when you need to restore your Quality Management system from the backup files due to a database corruption or some other problem.

TASK

1. Close Quality Management Administrator.
2. Stop the following services for Quality Management:
 - DB Cleaner service
 - DB Proxy service
 - MANA service
 - Sync service
 - Upload Controller service
 - Network Recording service
 - Monitor service
 - Jetty on the Site Upload server and the Base server
 - MediaSense Subscription service
3. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.
 - a. Right-click the database name (SQMDB) under the Databases node.
RESULT: A menu appears.
 - b. Choose Tasks > Restore > Database.
RESULT: The Restore Database window appears.
 - c. Complete the fields and click OK.
4. Restart the services for Quality Management you stopped in [step 2](#).

Genesys Connector Properties File Disaster Recovery

If you are using the Calabrio Genesys Connector, you need to create a backup of the qmgc.properties file before upgrading your system or for general disaster recovery purposes.

NOTE: A backup of the Genesys Connector properties file is not required if you are only using MediaSense Recording.

The qmgc.properties file is located in the ..\Calabrio\WFO_QMGenConnecor\config folder. Back up the file to a folder on the computer that hosts the Genesys Connector.

To restore the qmgc.properties file, copy the file from the backup folder to the ..\Calabrio\WFO_QMGenConnecor\config folder.

Index

A

Active Directory 94
 configuration guidelines 95
 domain name 96
Advanced Quality Management license 24, 25
automated package distribution tools 198
Automated Update feature 169

B

backup 207
backup and restore 207

C

Calabrio ONE 18
Calabrio Screen Player Plug-in 17
CDR information formats 161
Choose Monitor Adaptor 187
Cisco Unified CC database 134
Cisco Unified CCX database 134
Cisco Unified CM 140
client applications 17, 193, 200
codecs, required 65
Compliance Recording Application license 24
Compliance Recording license 24
components 17
concurrent users 32
Configuration Setup 125
contact reconciliation 20
Create Database Catalogs 187
CTI Manager 140
CTI service 22

D

data configuration environment 29

DB Cleaner service 19
Desktop Recording service
 about 17
 network interface cards (NICs) 52
 phone configurations 53
 requirements 51
disaster recovery 207
Display Metadata Encryption Key 187
Download /Install JTAPI 187

E

email addresses 156
Encrypt Audio Files 187
enterprise settings 148, 149
external storage 97, 191

F

firewall requirements 43

G

Generate Info for MSI Clients 187
Generate SSL Certificates 187

H

hardware VPN 54

I

inclusion list 171
installation status 183
IP phones
 supported 66

J

Jetty service 19

L

license 151
 importing 152
 licensing rules 151
 license type 23
 Live Monitoring
 consideration 56, 59

M

MANA service 19
 MediaSense Recording 61
 Microsoft SQL Server
 maintenance plans 89
 Microsoft SQL server 88
 Microsoft SQL Server Browser 91
 Microsoft Windows Server
 guidelines 87
 Monitor service 20
 monitoring and notification 149
 Monitoring and Recording Administrator 17

N

named users 32
 network interface cards (NICs) 52
 Network Recording
 considerations 51
 Network Recording service 20

P

patches 170
 PostInstall.exe 125

Q

Quality Management database 132

R

remote agent
 supported configurations 54, 58, 61
 Remove Recording 187
 removing Monitoring and Recording 203
 restore 207

S

server capacity guidelines 32
 Server Recording
 considerations 51
 services 18
 session timeout options 162, 163
 Set Recording Home Directory 187
 SIP trunk certificate 187
 SMTP settings 158
 SNMP settings 159
 software updates 169
 Start Local Services 187
 Sync service 20
 System Configuration Setup tools 186
 system requirements 29

T

Test CTI Service(s) 187

U

Update Mode 125
 upgrade status 183
 upgrades 110
 Upload Controller service 20

W

web applications 18