Cisco Unified Workforce Optimization

Quality Management Installation Guide Version 11.5

First Published: July 28, 2016

Last Updated: October 29, 2019

Cisco Systems, Inc. www.cisco.com

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.

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.

Installation Guide

Contents

Introduction

This document explains how to install Cisco Unified Workforce Optimization Quality Management 11.5 on a server in a Cisco Unified Contact Center Express (Unified CCX) environment.

For information on understanding the Quality Management system, the Unified CCX environment, architecture, components, capture and recording methods, and resiliency options, see the *Design Guide*.

What's New in This Version

Release 11.5(1)

Quality Management includes the following new features.

- Support for WebM screen recording
- Added requirement for FFMpeg on the servers where Media Encoder service is installed
- Added ability to import and export VoIP Devices in CSV format to the VoIP Devices table
- Added ability to assign Associated Call ID, Contact ID, and ICM Call ID call identifier options to a survey from the Post-Call Survey API
- Comments can now be applied to the entire form, a specific section, or a specific question on an evaluation form
- Added the Coach Panel to the evaluation form
- Added Surveys All Data and Survey Form Scores reports
- Add the ability to specify the AXL provider in the Unified CM Configuration dialog box
- Added support for the Import Calls API
- Added support for cloud-based recording storage
- Added the Screen Converter utility to convert screen recordings from REC format to M4V format
- Users can generate and manage their own encryption keys
- Users can untag calls that had been previously tagged for retention
- Users must use their own system administrator credentials to configure changes in the Admin API instead of using generic credentials built into the product
- Added CSRF token authentication to the Recording API

- Improved search capability from the VoIP Devices table in Monitoring and Recording Administrator
- Administrator roles are now selected from the Roles panel in the User Administration window
- Evaluator role has new configuration options
- Added options to address screen flashing issue when using Live Screen Monitoring
- All Managers Evaluate and All Supervisors Evaluate check boxes removed from the Evaluation and Approval Settings in Evaluation Form Administration
- Mark for Quality, Mark for Training, and Mark for HR options have moved to Media Player
- Added Kerberos Authentication to the Enterprise Server Settings window
- Removed most requirements for ActiveX
- Removed support for REC screen recording
- Removed the requirement for Proxy Networks software
- QM authentication can now use OpenLDAP (Lightweight Directory Access Protocol) to bind with standard LDAP servers and query for users. Full user management functionality may be limited by your LDAP directory architecture.
- QM now supports Cisco IP Communicator phones (phones with the IPC prefix) for desktop recording.
- Administrators can designate the time zone in which an agent’s contacts are recorded. QM displays this time zone in the agent’s contacts.
- Administrators can specify whether contacts can be tagged for training. If tagging of contacts for training is allowed, all agents can view these contacts.
- Users can change the speed at which the Media Player plays back contacts. The speed the contact is played back can vary from .5x (slower) to 3x (faster). The audio, screen, and position location on the energy bar are kept in sync when the playback speed is changed.
- When specifying goals for contact evaluations, administrators can define ranges of dates when the goals are effective, and when contacts are selected. This provides administrators with greater flexibility in how and when evaluation goals are assigned.
- Bug fixes

Release 11.5(1) SR5

- Quality Management version 11.5(1) user interface localized inChinese (simplified), Chinese (Traditional), Danish, Dutch (Standard), English (US), French (European), French (Canadian), German, Italian, Japanese, Korean, Portuguese (Portugal), Portuguese (Brazil), Russian, Spanish (International/Neutral), and Swedish.
- Bug fixes

Release 11.5(1) SR6

- Support for Cisco Unified Contact Center Express 11.6
- Added field to the Workflow Administration window that allows after call work recording to stop when a new call begins.
- Bug fixes

Release 11.5(1) SR7

- Bug fixes

System Requirements

The following topics list the minimum system requirements for Quality Management.

Quality Management Environment

Quality Management 11.5 is compatible with Cisco Workforce Management (WFM) 11.5.

Supported Environments

Environment	Version
Cisco Unified Contact Center Express	10.0, 10.5, 10.6. 11.0, 11.5, 11.6, 12.0
Cisco Unified Communications Manager	10.5, 10.5(1)SU2a, 10.5(2), 10.5(2)SU1,11.0, 11.5, 12.0
Cisco MediaSense	10.0, 10.5, 11.0, 11.5
Cisco Phone Model Support	Unified CM Silent Monitoring/Recording Supported Device Matrix
VMware ESXi	5.0, 5.1, 5.5, 6.0, and 6.5

HDD Partitioning

The recommended hard drive disk partitioning for the servers that host Quality Management are described in the following table.

Server	Hard Disk Partition	Size
Quality Management servers	Operation system partition (Windows OS)	32 GB minimum
	Application partition (Quality Management and SQL binaries)	40 GB (5 GB for the SQL installation)
	(Optional) Temporary storage partition (Daily Recording Storage)	

(Optional) Database Partition (SQL Database Server database and log files) **Note:** Only applies if the SQL application is co-resident with the Web Base server.	100 GB (30 GB for the database, 70 GB for the logs)
(Optional) Permanent storage partition (Permanent storage drive)	

Quality Management SQL server	Operation system partition (Windows OS)	32 GB minimum
	Application partition (SQL server binaries)	20 GB (5 GB for the SQL installation)

(Optional) Database Partition (SQL Server database and log files) **Note:** Only applies if the SQL application is co-resident with the Web Base server.	100 GB (30 GB for the database, 70 GB for the logs)

QM Versions 10.0, 10.5, 11.0, and 11.5

QM All in ONE (QM, Recording, and SQL) OVA

The QM All in One OVA provides a single server solution that includes the recording service for voice recording sessions via Server Recording (SPAN), Network Recording “Built-in Bridge”, MediaSense Recording, and Gateway (CUBE) Recording including a SQL Server database instance.

Specifications	2 vCPU	4 vCPU	6 vCPU	8 vCPU
Maximum concurrent recording service sessions[1]	25	100	300	400
vCPU	2	4	6	8

[1] Concurrent recording service sessions are tested for the amount of concurrent recording sessions while also monitoring 3 times that amount in active calls. “Monitoring” active call sessions entails registering a device for JTAPI events but not necessarily recording that device. Testing this way allows you to perform additional load testing on the Quality Management CTI service with respect to active recordings.

Specifications	2 vCPU	4 vCPU	6 vCPU	8 vCPU
Minimum Processor Speed	2 GHz	2 GHz	2 GHz	2 GHz
vRAM	4	4	6	8
Minimum input/output operations per second (IOPS)	143	143	143	143
HDD Partitioning				
System Storage (GB) for Operating System	32 GB	32 GB	32 GB	32 GB
Application Storage (GB) (QM/SQL Binaries)	40 GB	40 GB	40 GB	40 GB
SQL Database Partition (mdf, ldf) Note: Only applies if SQL is coresident with Quality Management.	100 GB	100 GB	100 GB	100 GB
Optional daily storage partition	See *Daily Recording Storage*	See *Daily Recording Storage*	See *Daily Recording Storage*	See *Daily Recording Storage*
Optional permanent storage partition	See *Permanent Recording Storage*	See *Permanent Recording Storage*	See *Permanent Recording Storage*	See *Permanent Recording Storage*

Concurrent recording sessions—the maximum number of concurrent recording sessions over a period of 24 hours for the QM recording service.

Concurrent active calls—the maximum number of device calls actively being monitored via JTAPI registration by the QM CTI Service.

> **Example:** If you are monitoring JTAPI events for 75 active calls over a period of 24 hours, the maximum number of concurrent recording sessions handled by the recording service is 25.

Expansion Recording Server OVA

You can add expansion Recording servers to an existing QM All in one OVA to increase recording capacity.

Specifications	2 vCPU	4 vCPU	6 vCPU	8 vCPU
Maximum concurrent recording service sessions[1]	150	300	500	600
vCPU	2	4	6	8
Minimum Processor Speed	2 GHz	2 GHz	2 GHz	2 GHz
vRAM	4	4	6	8
Minimum input/output operations per second (IOPS)	143	143	143	143
HDD Partitioning				
System Storage (GB) for Operating System	32 GB	32 GB	32 GB	32 GB
Application Storage (GB) (QM/SQL Binaries)	40 GB	40 GB	40 GB	40 GB
Optional daily storage partition	See *Daily Recording Storage*	See *Daily Recording Storage*	See *Daily Recording Storage*	See *Daily Recording Storage*
Optional permanent storage partition	See *Permanent Recording Storage*	See *Permanent Recording Storage*	See *Permanent Recording Storage*	See *Permanent Recording Storage*

IOPS and Storage System Performance Requirements

The minimum IOPS for QM 9.0 and later is 143.

Cisco WFO Desktop Recording

Desktop Recording is a recording method where a recording client application is installed on a client desktop to capture packets of an IP phone that is daisy chained to the client desktop. Desktop recording can be used in addition to any of the existing OVA designs which may use the Recording

[1] Concurrent recording service sessions are tested for the amount of concurrent recording sessions while also monitoring 3 times that amount in active calls. “Monitoring” active call sessions entails registering a device for JTAPI events but not necessarily recording that device. Testing this way allows you to perform additional load testing on the Quality Management CTI service with respect to active recordings.

Service for Server Recording (SPAN), Network Recording “Built in Bridge”, MediaSense Recording, or Gateway (CUBE) Recording.

Daily Recording Storage

You need to determine your hard disk space requirements for the daily recording storage. Daily recording storage is where the recording service will store recorded files temporarily until they are uploaded to permanent storage. The formula used to determine hard disk space requirements, in GB, for a single recording server configuration is as follows:

The daily recording storage requirements are as follows:

- For 8-bit WAV—the value is 2 GB for voice recording only or 2.5 GB for voice and screen recording
- For 16-bit WAV—the value is 6 GB for voice recording only or 6.5 GB for voice and screen recording

Daily Recording Storage Formula:

- C= GB
- D= Number of Recording users

Daily Storage = C x D

Example: (.5 GB x 100 Recording users) = 50 GB Daily Storage

Permanent Recording Storage

To calculate the storage that required for your contact center, 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	File Format	Formula
Daily recorded minutes		(# of Agents) × (Avg. call length) × (# of Calls) = Daily Recorded Minutes
Total recorded minutes to store		(Daily Recorded Minutes) × (Days per Month) × (Months to store) = Stored
Voice recording storage (MB)	SPX	Stored = 0.12 MB/Minute = Voice
	8-bit WAV	Stored = 0.48 MB/Minute = Voice
	16-bit WAV	Stored = 1.44 MB/Minute = Voice
Note: The storage requirement for screen recording depends 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.		Stored = 1.20 MB/Minute = Screen

Cisco WFO QM OVA Design Examples

The following examples show how to scale Quality Management by adding a separate Expansion Recording Server OVA when Quality Management reaches its recording capacity. This applies to all three QM All in ONE OVA solutions.

Example 1–All in one 2 vCPU OVA with Expansion Recording server	
OVA Description	**Concurrent Users**
2 vCPU QM all in one OVA (includes SQL server)	25 for Network Recording
2 vCPU Expansion Recording server OVA	150 for Network Recording
Total concurrent recording users	175 for Network Recording

Example 2—All in one 4 vCPU OVA with Expansion Recording server	
OVA Description	**Concurrent Users**
4 vCPU QM all in one OVA (includes SQL server)	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
Total concurrent recording users	400 for Network Recording

Cisco WFO QM OVA Design Examples

The following examples show how to scale Quality Management by adding a separate Expansion Recording Server OVA when Quality Management reaches its recording capacity. This applies to all three QM All in ONE OVA solutions.

Example 1—All in one 2 vCPU OVA with Expansion Recording server	
OVA Description	**Concurrent Users**
2 vCPU QM all in one OVA (includes SQL server)	25 for Network Recording
2 vCPU Expansion Recording server OVA	150 for Network Recording
Total concurrent recording users	175 for Network Recording

Example 2—All in one 4 vCPU OVA with Expansion Recording server	
OVA Description	**Concurrent Users**
4 vCPU QM all in one OVA (includes SQL server)	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
Total concurrent recording users	400 for Network Recording

Example 3—QM + Recording server OVA + Standalone SQL server	
OVA Description	**Concurrent Users**

Example 3—QM + Recording server OVA + Standalone SQL server	
4 vCPU QM all in one OVA	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	400 for Network Recording

Example 4—Redundant CTI with Standalone SQL server	
OVA Description	**Concurrent Users**
4 vCPU QM all in one OVA	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
2 vCPU QM all in one OVA (Redundant CTI server)	N/A
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	400 for Network Recording

Example 5—Redundant CTI and Recording servers with Standalone SQL server	
OVA Description	**Concurrent Users**
6 vCPU QM all in one OVA	300 for Network Recording
6 vCPU Expansion Recording server OVA	500 for Network Recording
6 vCPU Expansion Recording server OVA (Redundant Recording server)	500 for Network Recording
2 vCPU QM all in one OVA (Redundant CTI server)	N/A
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	800 for Network Recording

Example 3—QM + Recording server OVA + Standalone SQL server	
OVA Description	Concurrent Users
4 vCPU QM all in one OVA	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	400 for Network Recording

Example 4—Redundant CTI with Standalone SQL server	
OVA Description	Concurrent Users
4 vCPU QM all in one OVA	100 for Network Recording
4 vCPU Expansion Recording server OVA	300 for Network Recording
2 vCPU QM all in one OVA (Redundant CTI server)	N/A
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	400 for Network Recording

Example 5—Redundant CTI and Recording servers with Standalone SQL server	
OVA Description	Concurrent Users
6 vCPU QM all in one OVA	300 for Network Recording
6 vCPU Expansion Recording server OVA	500 for Network Recording
6 vCPU Expansion Recording server OVA (Redundant Recording server)	500 for Network Recording
2 vCPU QM all in one OVA (Redundant CTI server)	N/A
4 vCPU QM all in one OVA for Standalone SQL server	N/A
Total concurrent recording users	800 for Network Recording

Server Operating Systems

Quality Management supports 64-bit Windows Server 2008 R2, 2012, 2012 R2, and 2016.

> **Note:** Since Quality Management does not have direct version/update dependencies, it is permissible to apply updates to the server operating system as recommended by Microsoft.

> **Best Practices:** If you install Wireshark on a Monitor server or a Media Monitor server where Windows 2012 or 2012 R2 is installed, you must disable WinPcap at startup and restart the server to ensure that Wireshark and Quality Management services will both work simultaneously.

Microsoft SQL Server

Microsoft 64-bit SQL Server 2008, 2008 R2, 2012, 2014 and 2016.

When determining your Microsoft SQL server requirements, note the following:

- Quality Management only supports the Express Edition for smaller customer sites where the number of recorded contacts in the database are equal to or less than 500,000. If the number of recorded contacts is greater than 500,000, Microsoft SQL Server Standard edition is required at minimum.
- The Express Edition of the Microsoft SQL server has the following limitations:
  - Supports only 1 CPU (dual/quad cores count as 1).
  - Limited to 1 GB RAM. This affects large databases.

    > **Note:** The size limitation can affect paging in large databases.

  - SQL Profiler is not included in the Express Edition. Cisco's ability to troubleshoot performance issues will be limited.
- The NTRights utility (ntrights.exe), available in the Windows Resource Kit, is required to grant the external storage user Log on as a Service rights. For more information, see http://support.microsoft.com/kb/315276.
- To install the Monitor Server on a SQL Server 2008 R2 machine, you will need to install two KB patches: KB2921916, and KB3033929. For more information, see these websites:

https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2921916&kbln=en-US

https://www.microsoft.com/en-us/download/details.aspx?id=46148

Microsoft SQL Server Licensing

The Per Core licensing model is appropriate when:

- Deploying the SQL Server 2012 Enterprise or Parallel Data Warehouse editions.
- Deploying Internet or extranet workloads, systems that integrate with external-facing workloads (even if external data goes through one or more other systems), or when the number of users/devices cannot be counted easily.
- Implementing centralized deployments that span a large number of direct and/or indirect users/devices.
- The total licensing costs are lower than those incurred using the Server+CAL licensing model.

> **Note:** The use of hyper-threading technology does not affect the number of core licenses required when running SQL Server software in a physical OSE.

The Server+CAL licensing model is appropriate when:

- Deploying the SQL Server Business Intelligence Edition.
- Deploying SQL Server Standard Edition in scenarios where you can easily count users/devices and the total licensing costs are lower than using the Per Core licensing model.
- Accessing multiple SQL Server databases and/or planning to scale out the use of SQL Server by adding new servers over time. Once you have purchased the necessary CALs, you only need to purchase low cost server licenses for new server system deployments.
- Accessing “legacy” Enterprise Edition servers in the Server+CAL licensing model.

Virtual Server Environment

A virtual server environment requires hardware resources equivalent to those required for a physical server for a given number of users (see *System Requirements*). Quality Management must be installed in its own computing environment that is not shared with multiple hosts.

Quality Management supports WMware ESXi 5.0, 5.1, and 5.5.

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 signaling service or running a service restart script.

The recommended VMWare settings are as follows:

Setting	Description
Shares	Guarantee that VMs are given a percentage of an available resource (CPU, RAM, Storage I/O, Network)
Limits	Guarantees that a VM does not consume more than a specified resource limit
Resource Reservation	Provides an allocated resource for a VM on startup.

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

Exchange

Exchange	Version
Microsoft Exchange Server	2007, 2010, 2013
Microsoft Office	365

Event Timestamps

Many features within Quality Management rely on timestamps of events to properly associate data with the correct person or call. Quality Management requires that all servers running Cisco software are configured to use the same Network Time Protocol (NTP) server as Cisco Unified Communications Manager. Windows Time Service is one method that can be used for this purpose.

The agent's timestamp for a call depends on where the call is recorded.

- Desktop Recording—The call is recorded on the agent's desktop so the timestamp and time zone for the call will be associated the agent's desktop.
- Recording Server—The call is recorded on a Recording Server so the timestamp and time zone for the call will be associated with the Recording Server. If the agent is in one time zone and the Recording Server is in another timezone, the timestamp and time zone for the call will be associated with the Recording Server. If you have multiple Recording Servers and they are in different time zones, the timestamp and time zone used will be based on where each Recording Server is located.

Recording Export

After installing 11.5, you must also install FFmpeg on the servers where the Media Encoder service (MediaEncoder.exe) is installed. FFmpeg is required when you export recordings from Cisco. See *Install Services on a Single Server* for installation requirements.

Single Web Base Server Capacity Guidelines

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

Note: Refer to *System Requirements* for the specifications for Ultra, Large, Medium, and Small servers.

	Server Type			
	Ultra Server	Large Server	Medium Server	Small Server
Maximum number of named users for voice and screen recording **Note:** If the number of named Users exceeds 10000 it will require a custom design and must be reviewed by Cisco PDI.	10000	5000	2500	1000

	Server Type			
	Ultra Server	Large Server	Medium Server	Small Server
Maximum number of registered devices in a subscription service **Note:** You can double the number of registered devices if the subscription service is installed on a separate dedicated server.	5000	2500	1250	600
Maximum number of concurrent agents for MediaSense Recording, Server Recording, Network Recording, Network Based Recording, or Gateway Recording (always voice, no screen option)	500	150	60	25

When determining your base server requirements, remember the following points:

- The most desirable configuration uses a large, medium, or small server. Use an ultra server only when the number of named users exceeds 10000 and you cannot use multiple smaller servers.
- The capacity guidelines shown above assume all services required for a single server configuration are installed on the base server, including Web Base Services, Database Services, the signaling service, and Site Upload Server. You can choose to off-load the Database Services, signaling service, and Site Upload Server to other servers to improve capacity for a specific service.

  Example: Install the signaling service or the Site Upload Server on another server.

- An ultra server requires VMware ESXi 5.1 or higher if you are going to use it as a virtualized server.
- If you install the CTI service and the MediaSense Subscription service on the same server you have to either double your concurrent user number or halve your capacity.

To determine the capacity requirements for your base server:

1. Compare your number of named users to the table above to determine the server size.

   > **Example:** If your site requires between 2501 and 5000 named users on your base server, you need a large server.

2. Compare your number of concurrent users to the server size determined by your number of named users.

   > **Example:** If the number of concurrent users is less than or equal to 150, the signaling service can remain on the large server. If the number concurrent users exceeds the maximum allowed for the server, it is recommended that you move the signaling service to another server. Note that if you move the signaling service to another server, it can handle **twice** the number of concurrent users. So you could move the signaling service to a medium server without effecting the number of concurrent users required for your configuration.

See Recording Storage Requirements for additional information on storage requirements and external database requirements.

Recording Server Capacity Guidelines

The system capacity for a Recording Server is determined by your hardware, as well as the number of users.

The users are defined as follows:

- Concurrent users—The users who are logged in at any given time.
- Configured or named users—The users who are configured and licensed

  > **Example:** agents, supervisors, managers, evaluators, and archive users

Recording Format	Specifications	Ultra Server	Large Server	Medium Server	Small Server
SPX	Audio Media File Storage (GB)	500	125	100	100
	Concurrent Users	1000	300	125	50
8-bit WAV	Audio Media File Storage (GB)	2000	500	400	400
	Concurrent Users	1000	1000	1000	500

Recording Format	Specifications	Ultra Server	Large Server	Medium Server	Small Server
16-bit WAV	Audio Media File Storage (GB)	6000	1500	1200	1200
	Concurrent Users	1000	1000	500	200
All Recording Formats	Minimum IOPS	429	143	143	143

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

When determining audio media file storage, consider the following.

Note: 8-bit WAV is uncompressed and the files are four times the size of a compressed SPX file. 16-bit WAV has higher audio quality, is uncompressed, and is 12 times the size of a compressed SPX file.

- Recording storage varies by use.
- The temporary recording location on a Recording 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.

EXAMPLE 1: If you are using the SPX recording format and you have 432 concurrent agents in a single server configuration, you need an ultra server. There is no resiliency with a single ultra server. If you want resiliency, add another ultra server.

EXAMPLE 2: If you are using the SPX recording format and have 132 concurrent agents in a single server configuration, you can use one large server. There is no resiliency with a single large server. If you want resiliency, add another large server.

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)	SPX	Stored × 0.12 MB/minute = Voice
	8-bit WAV	Stored × 0.48 MB/Minute = Voice
	16-bit WAV	Stored × 1.44 MB/Minute = Voice
Screen recording storage (MB) **Note:** The storage requirements for screen recordings depend on two factors: screen activity and monitor resolution. The number is based on a single screen. The value shown here is based on moderate to high screen activity, 1920 × 1080 resolution, and a single monitor. This rate may increase by 50% when recording dynamic, graphical, or media-intensive applications. Each screen will increase this requirement by the same size. For example, if you record three screens for three minutes the storage requirements will be approximately 4.5 MB × 3 for a total of 13.5 MB.		Stored × 1.50 MB/minute = Screen

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. The retention time for recordings is set withing the Quality and Archive workflows.

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 audio recordings remain on the recording service and the screen recordings remain on the client PC 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 Recording 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 Recording Server. The formula used to determine hard disk space requirements, in GB, for a single server configuration is as follows:

```
A + B + (C × D)
```

where:

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

B = Database (The value is 100 GB and includes both database and transaction logs.)

C = GB

- For SPX—the value is .5 GB for voice recording only or 1 GB for voice and screen recording
- For 8-bit WAV—the value is 2 GB for voice recording only or 2.5 GB for voice and screen recording
- For 16-bit WAV—the value is 6 GB for voice recording only or 6.5 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 Recording Server.

Example: `40 + 100 + (0.5 × 100) = 190 GB`

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

`A + (C × D)`

Example: `40 + (0.5 × 300) = 190 GB`

Recording Storage Requirements

The recording storage requirements are as follows:

- Voice recording only:
    - SPX—.5 GB/recorded user
    - 8-bit WAV—2 GB/recorded user
    - 16-bit WAV—6 GB/recorded user
- Voice and screen recording:
    - SPX—1 GB/recorded user
    - 8-bit WAV—2.5 GB/recorded user
    - 16-bit WAV—6.5 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 server where the services are installed.

NOTE: The recordings must be stored on a local drive. You can only specify a network drive if your are using a virtual machine.

If you plan to use cloud-based storage for recordings, you must install the CloudBerry Drive Server on each Site Upload server. The CloudBerry Drive server is available at:

http://www.cloudberrylab.com/amazon-cloud-server-drive.aspx.

When configuring CloudBerry, you need to:

- Ensure that the File cache directory has enough space during uploads.
- Create a storage account using your credentials and S3 bucket location.

- Add a mapped drive using the storage account your created in the previous step. The volume label must be a unique name since it is the Windows share name used when configuring Quality Management.
- Set the path to the S3 storage bucket location that will be uses as the root for the Quality Management storage location.
- Select the Mount this account as virtual disk at system startup check box.
- Ensure Quality Management has read and write access.
- Mount as Network Mapped Drive and select the Allow access from other computers via network share.

Quality Management uses CloudBerry Drive to upload the files to the virtual network drive. That drive will actually write the data to this cache directory and then slowly upload files in the background. The file is successfully uploaded as soon as it is written to the cache directory. If Quality Management tries to upload files faster than the virtual drive can upload files to the S3 bucket, or if the virtual drive looses its connection to the S3 Storage, this directory will grow.

Bandwidth Usage

Cisco supports 30 KB per second bandwidth for screen recording and playback.

The following table displays the transfer bitrate by recording format.

Recording Format	SPX	8-bit WAV	16-bit WAV
Format	8000 Hz variable bit pulse-code modulation (PCM)	8000 Hz 8-bit PCM	8000 Hz 16-bit PCM
Transfer Bitrate		64 kbits/s	128 kbits/s
KB/Minute		469 KB	938 KB
File Transfer Type	WAV-16	WAV-8	WAV-16

For additional information on bandwidth usage, see "IP Call Bandwidth Usage" in the *Cisco Unified Contact Center Express Solution Reference Network Design* on the Cisco website (www.cisco.com).

Contact Metadata and the Microsoft SQL Server

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 × B × C × 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

Example: `300 × 25 × 22 × 13 = 2.1 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 the following table must be available and configured for use by Microsoft SQL on its hosting server. For deployments where Microsoft SQL is coresident with the Web Base Services, you can dedicate a maximum of 1 CPU Core and 2 GB RAM to Microsoft SQL from the server resources for physical server hardware requirements.

Example: Microsoft SQL is coresident with the Web Base services in a single server architecture or Cisco Unified Computing System (UCS) environment.

The following table 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 or processing threads, so the number of recommended cores for AMD are doubled when compared to Intel. *System Requirements* provides a breakdown of processors, cores, and threads.

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

Specifications	Ultra	Large	Medium	Small
Dedicated Memory for Microsoft SQL Server	12 GB RAM[1]	8 GB RAM	6 GB RAM	2 GB RAM
Requires an Off-board Microsoft SQL Server	Yes	Yes	Yes	No

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.

SQL Server Guidelines and Contact Metadata

The contact metadata for Quality Management is stored in Microsoft SQL database server. To ensure satisfactory response rates from the Microsoft SQL database the resources listed in the following table must be available and configured for use by Microsoft SQL on its hosting server.

Standalone SQL Server

You have the option to deploy a standalone Microsoft SQL Database server to improve response rates and allow for scalability. If you choose to implement a standalone SQL Server then use the QM All in One OVA template for the purpose of SQL Server deployment. Determining vCPU requirements should be based on your Contact Metadata calculations (call volumes, retention periods, number of agents, and so on).

Increasing vRAM for SQL

You can also scale RAM in increments of 2 GB for the SQL Server as the number of contact metadata increases. This will ensure satisfactory response rates from the Microsoft SQL Server database. Please reference the table below for guidelines. This applies to coresident SQL in QM All in One OVA and the standalone SQL Server deployments.

Use the following formula to estimate the maximum number of contacts stored in the database:

A × B × C × D = E

where:

- A = Number of agents
- B = Average number of recorded contacts per day per agent

[1] See *Determining Required RAM for the Microsoft SQL Server* if the number of saved contacts exceed 12 million.

- C = Number of days per month the contact center handles calls
- D = Configured retention time in months
- E = Total saved contacts in the database

Example: 300 (agents) x 25 (average, contacts/day) x 22 (# days/month) x 12 (retention months) = 2.1 million recorded calls (contacts in database)

Specifications	All in One System			Recording Server	
	2 vCPU	4 vCPU	6 vCPU	6 vCPU + 4 vCPU	6 vCPU + 6 vCPU
Number of Recording Users	25	100	300	400	600
Average number of recorded contact per day/per user	50	40	40	40	40
Number of days per month taking calls	22	22	22	22	22
Configured retention time in months	12	12	12	12	12
Example calculations of total saved contacts in the database based on OVA	264,000	1,056,000	3,168,000	4,224,000	6,336,000
Total saved contacts in the database	Less than 500,000 contacts	500,000 - 2 Million contacts	2 - 4 Million contacts	4,000,000 + contacts	6,000,000 + contacts
Minimum SQL Edition	SQL Express (up to 500K Contacts) or SQL Standard Edition—see below for additional information	SQL Standard Edition	SQL Standard Edition	SQL Standard Edition	SQL Standard Edition

Specifications	All in One System			Recording Server	
	2 vCPU	4 vCPU	6 vCPU	6 vCPU + 4 vCPU	6 vCPU + 6 vCPU
Requires an Off-board Microsoft SQL Server	No	No	No	Yes	Yes
Optional Standalone Microsoft SQL Server	Use 2 or 4 vCPU QM All in One OVA	Use 2 or 4 vCPU QM All in One OVA	Use 4 or 6 vCPU QM All in One OVA for SQL	Use 4 or 6 vCPU QM All in One OVA for SQL	Use 6 vCPU QM All in One OVA for SQL

You can use Microsoft SQL Server Express if the overall number of Cisco WFO contacts in the database is less than 500,000 contacts, and the following Microsoft SQL Express limitations are not exceeded:

- Limited to lesser of 1 Socket or 4 cores
- Maximum 1 GB RAM
- Maximum database Size 10 GB

Determining Required RAM for the Microsoft SQL Server

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

`A ÷ 2 = B`

where:

A = Number of Million Contacts Saved

B = Number of Gigabytes RAM

Example: `110 ÷ 2 = 55 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.

Deploying Analytics Automated Pause and Resume

If you plan to deploy and configure the Automated Pause and Resume feature for use with Advanced Quality Management please follow the installation guidelines referenced in the *Analytics Installation guide*. The following table lists the required server specifications when only using the Automated

Pause and Resume component with Advanced Quality Management. If you plan on deploying and using Unified Workforce Optimization Analytics as a full application, please refer to the *Analytics Installation Guide* and *Analytics Administration* for a full deployment and design requirements.

Processor	■ Intel: Xeon Processor E3 family or higher running above 2 GHz or Xeon Processor 5502 on up with hyper threading (Required) ■ AMD: Opteron Processor 3000 or higher
Processor cores	2
Minimum processor speed	2 GHz
Memory	4 GB
System Storage	80 GB (This is for the operating system and Automated Pause and Resume)

Supported Third Party Software

Zeranoe FFmpeg—FFmpeg is required when you export recordings from Cisco Quality Management. Download the 64-bit static FFmpeg from http://ffmpeg.zeranoe.com/builds/.

Note: When you navigate to the FFmpeg URL above, be sure to select and download the most recent stable release.

Adobe Acrobat Reader 6.0 or later—Acrobat Reader is required to open PDF-based reports and user documentation. A free Acrobat Reader download is available at www.adobe.com.

Important: By default, Adobe Reader enables an Enhanced Security feature that prevents Desktop Analytics from detecting that a user is viewing a document in Adobe Reader. If your business needs require tracking Adobe Reader usage, you must lower the security settings for Adobe Reader. To do this, start Adobe Reader and choose Edit > Preferences > Security (Enhanced). Clear the Enable Protected Mode at startup and Enhanced Security check boxes, click Yes for any warning messages that might appear, and then click OK to save your changes. When finished, restart Adobe Reader for the changes to take effect.

If you are running antivirus software you might need to create exceptions for the Quality Management installation directory and both temporary and permanent storage locations.

After you install Analytics, copy the filecryptokeystore file from its installed location to each server where the Retrieval service is installed. If this is not done, you will not be able to use Analytics to index customer conversations. See *Install the Filecryptokeystore File* for instructions.

Desktop Requirements

These desktop hardware requirements apply to Recording and Quality Management.

PC Hardware	
Memory	2 GB RAM
CPU	Intel Core 2 Duo 2.0 GHz, Core i3, AMD Athlon 64 X2 or better
NIC	100 Mbit NIC NICs must support Promiscuous Mode.
Disk Space	Screen storage formula: # of Recordings x Avg Call Length x 1.20 MB/Minute = MB of Required storage per day **Note:** The storage requirements for screen recordings depend on three factors: recording length, monitor resolution, and the number of monitors being recorded. The value shown here is based on a single monitor. Each additional monitor is recorded separately; apply this formula for each monitor.

These operating system requirementsapply to Recording and Quality Management.

Product	Operating System
	■ Windows 10–with Windows Internet Explorer 11 (32-bit), Desktop mode ■ Windows 8.1 (32/64-bit)–Professional Windows Media Player is required. Only Windows 8.1 Volume License (VL) includes Windows Media Player. For all other versions of Windows 8.1, you must download and install the Media Feature Pack for Windows 8.1 separately to add Windows Media Player. **Note:** Quality Management does not support Wireshark on Windows 8.1. ■ Windows 7 (32/64-bit)–Professional, Enterprise, Ultimate Windows Media Player is required. Windows Media Player is not included in Windows 7 N or KN. If you are using Windows 7 N or KN, you must download and install Windows Feature Pack for Windows N and KN separately to add Windows Media Player. **Note:** Cisco supports the operating system's latest Service Pack.

Windows Aero Theme

Windows Aero theme is not supported by the Desktop Recording service.

Live screen monitoring is based on the Microsoft Windows Desktop Sharing API. This same API is used by Microsoft Windows Remote Assistance. One limitation of the Microsoft Windows Desktop Sharing API is that it does not support the Windows Aero theme for the PC running the Desktop Recording service. Every time the Desktop Recording Service starts, Windows will automatically switch your PC to the Windows Basic theme. The Windows Basic theme will remain until the Desktop Recording service is stopped.

If this is not the desired behavior, choose one of the following work arounds:

- Configure your PC to always use the Windows Basic theme. Then when the QM Desktop Recording service starts it does not have to change to that theme since it is already in place.
- Disable the live screen monitoring feature in Monitoring and Recording Administrator by clearing the Enabled check box under Live Screen Monitor in the Interface Settings window under Recordings. This will disable live screen monitoring for all users. When live screen monitoring is disabled, it will not switch to the Windows Basic theme.

Browser

Unified Workforce Optimization supports the following browsers:

- Internet Explorer 11 (32-bit), Desktop mode
- Internet Explorer 10 (32-bit), Desktop mode
- Internet Explorer 9 (32-bit)

  Note: The Emulation mode for Internet Explorer must be Internet Explorer 9 or greater.

- Google Chrome—The Live Screen Monitoring feature on the Live Monitoring page requires the IE Tab extension from Google because it uses ActiveX.

Note: If your site requires an SSL certificate, the SSL certificate must be installed on the Web Base server by your administrator.

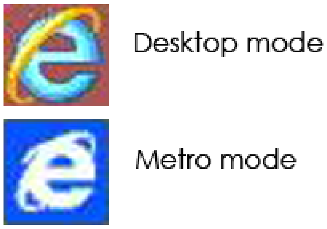
Note: The Report Viewer is not identically compatible with the supported browsers listed above. This affects the way reports are displayed in Report Manager and QM Reports. See the Microsoft Developer Network topic, “Planning for Reporting Services and Power View Browser Support (Reporting Services 2014)” (https://msdn.microsoft.com/en-us/library/ms156511%28v=sql.120%29.aspx) or “Browser Support for Reporting Services and Power View, SQL Server 2016 or later” (https://msdn.microsoft.com/en-us/library/ms156511.aspx) for more information.

Internet Explorer and Windows 8.1

By default, Windows 8.1 opens Internet Explorer 10 and 11 in the Metro mode. This mode is not supported in the Cisco Unified Workforce Optimization suite. All products in the Cisco Unified Workforce Optimization suite require that Internet Explorer be run in Desktop mode.

To run Internet Explorer in Desktop mode, pin it to the Windows taskbar and launch it from there.

You can identify which mode of Internet Explorer you are using by the icon that appears in the Windows taskbar:



Required Internet Explorer Options

The following options are required for all products in the Unified Workforce Optimization:

- File Downloads must be enabled
- Pop-up blockers must be disabled

GPO for PCI Compliance

Note: This information only applies to Quality Management.

If you apply a Group Policy Object (GPO) for Payment Card Industry Data Security Standard (PCI DSS) compliance to your browsers, include the following values to the settings in the Group Policy Management Editor:

- All Processes—Disabled
- Internet Explorer Processes—Enabled

Thin Client Requirements

- Citrix XenApp 4.5, 4.6, 5.0, 6.0, 6.5, 7.6
- Microsoft Terminal Services for Windows Server 2008 R2 and 2012 R2

Note: Recording and Quality Management only supports Citrix XenApp installed on the supported Windows Servers. See *Server Operating Systems* for more information.

When using a Thin Client, please note:

- Citrix XenApp or Microsoft Terminal Services using the Thin Client application requires a remote desktop session to record screen. If no remote desktop session is presented, alternatively installing the Desktop Recording Service will do screen recording on the desktop, including any XenApp applications.
- Use Immediate Screen Upload if you are using Thin Clients or non-persistent desktops.
- 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.
- If your virtual image has access to your local NIC, you can use the Desktop Recording Service for agent-side recording.

Note: If you are planning to use a virtual or Citrix environment, see *Virtual Server Environment* or Citrix or Windows Terminal Services for additional information.

Citrix XenApp or Windows Terminal Services

Install Citrix XenApp or Windows Terminal Services per the product documentation. When installing Citrix XenApp or Windows Terminal Services, use the following settings to support screen recording in Recording and Quality Management:

- Servers must include a supported browser to access the Unified Workforce Optimization Container.
  - Publish the browser locally to each server.
  - Ensure the security settings allows end users to play back recordings through Citrix XenApp 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 Unified Workforce Optimization Container. See the “Installing Server Applications” in the *Installation Guide* for complete details.
- Limit the number of simultaneous sessions per user to a single session.

- For Citrix XenApp, 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 XenApp requires the QmWmpAudioPlayer class
- On the server that hosts the Quality Management database, set the dbProperties flag in SQMDB to isCitrix

For Citrix client services, you must also install the Recording Thin Client. The Recording Thin Client records screens from Citrix XenApp Client sessions.

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

Desktop Applications

- Quality Management Administrator
- Desktop Recording service
- Recording Controls
- Recording Export (CRX) utility
- Microsoft Visual C++ 2013 Redistributable Package x86)

> **Note:** The Microsoft Visual C++ 2013 Redistributable Package is only required for managers and supervisors that want to use the Live Screen Monitoring feature.

Quality Management Port Usage

The following topics list the inbound port requirements for the Quality Management server components and the server connections to external integration points.

All outbound communications uses dynamic ports unless otherwise listed. A server may contain one or more components and not all ports are required for all recording types.

See *Windows Firewall or Internet Connection Sharing Service* for additional information on Microsoft SQL Server and Informix JDBC Driver ports.

Windows Firewall or Internet Connection Sharing Service

For Unified Workforce Optimization to function correctly, the ports listed in this document must be opened in Windows Firewall.

If Windows Firewall or the Internet Connection Sharing (ICS) service is running when Unified Workforce Optimization is installed, the installation process opens the necessary firewall ports except those in the following table, which must be opened manually.

Product	Open Manually
Quality Management	Microsoft SQL Server: ports 1433 and 1434 Informix JDBC Driver: port 1504 (Unified CCX environment only)

Ports must be opened manually in these situations:

- If another firewall is used
- If you turn on the Windows Firewall after Unified Workforce Optimization is installed

See your firewall documentation for instructions on configuring manual port exceptions.

Note: Any non-Unified Workforce Optimization services that use the ports listed in this document must be configured to use a different port.

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.

To allow the Microsoft SQL Server through the Windows Firewall:

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

   The Windows Firewall application starts.

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

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

3. Click the Allow Another Program button.

   The Add a program dialog box appears.

4. Click Browse and navigate to the Microsoft SQL Server engine (sqlserver.exe).

5. Click OPEN.

6. In the Windows Firewall window, verify that sqlserver.exe is in the list of Programs and click Add.

   All ports that the Microsoft SQL Server opens are now accessible.

Quality Management Jetty Component

The Monitoring and Recording Jetty service uses TCP ports 80, 443, and 7001. 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.

> **Example:** Microsoft SQL Server 2008 R2 Reporting Services and Microsoft Internet Information Services (IIS) might use these ports.

Port 7001 is reserved exclusively for Quality Management for encrypted data transfer.

The SQL Server 2008 R2 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.

Consult your SQL Server documentation for instructions on changing the port used by SQL Server 2008 R2 Reporting Services.

Base Component

The following table lists the inbound ports on the base server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
80	TCP	Jetty service (Jetty port)	All servers and clients
443	TCP	Jetty service (Jetty SSL port)	All servers and clients
7001	TCP	Jetty service (Jetty alternate port)	All servers and clients
59011	TCP	Sync service	Quality Management Administrator client
59103	TCP	Jetty service (Data API service) **Note:** 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.	Data API

External Communication (* indicates default port)

Port	Type	Destination	Source
1504	TCP	Unified CCX Informix database	Sync for Unified CCX
8443, 443, or 80	TCP	Unified CM Publisher and Subscribers	MANA, Sync, and Quality Management Administrator
389* or 636*	TCP	Active Directory	Data API and Quality Management Administrator
25*	TCP	SMTP Server	MANA and Jetty
*	TCP	SNMP	MANA
1433	TCP	SQL	System Configuration Setup (postinstall.exe), Data API, and Sync

Operations Base Component

The following table lists the ports on the operations server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
59011	TCP	Sync service	Quality Management Administrator client
443	TCP	Jetty service (Jetty SSL port)	All servers and clients
7001	TCP	Jetty service (Jetty alternate port)	All servers and clients

External Communication (* indicates default port)

Port	Type	Destination	Source
135 to 139 and 445	TCP	Storage Location	Jetty Service (file transfer)
1504	TCP	Unified CCX Informix database	Sync for Unified CCX
8443, 443, or 80	TCP	Unified CM Publisher and Subscribers	MANA, Sync, and Quality Management Administrator

CTI Component

The following table lists the ports on the recording CTI server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
2789	UDP	CTI Service	JTAPI config updates from CUCM
52102	UDP	CTI Service	All servers and clients
5060	UDP/TCP	CTI Service	Recording CTI service (SIP Messaging)
5061	TCP	CTI Service	Recording CTI service (secure SIP Messaging)
59110	TCP	CTI Service	AACC with MLS

External Communication (* indicates default port)

Port	Type	Destination	Source
1433*	TCP	SQL database	DB proxy
	TCP	Unified CM CTI Manager	CTI service

CUBE SIP CTI Component

The following table lists the ports on the CUBE SIP CTI server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
5060	UDP/TCP	CUBE SIP CTI service	CUBE Voice Gateway
59106	TCP	CUBE SIP CTI service	All servers

External Communication

None

MediaSense Subscription Component

The following table lists the ports on the MediaSense Subscription server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
59104	TCP	MediaSense Subscription service	All servers
59105	TCP	MediaSense Subscription service	All servers

Monitor Server Component

The following table lists the ports on the Monitor server that must be opened in the Windows Firewall for Server Recording deployments.

Inbound Ports

Port	Type	Destination	Source
59101	TCP	Monitor service	All servers
All	All	Monitoring NIC	SPAN Session

External Communication

None

Voice Record Component

If you are not using Windows Firewall, the following table lists the ports on the Recording Server that must be opened.

Inbound Ports

Port	Type	Destination	Source
59102	TCP	Network Recording service	All servers
39500 to 41500	UDP	Network Recording service	BiB RTP stream from phones or RTP stream from CUBE

External Communication (* indicates default port)

Port	Type	Destination	Source
8440*	TCP	MediaSense Recording Server	Recording Server

Site Component

The following table lists the ports on the Site Upload server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
80	TCP	Jetty service (Jetty port)	All servers and clients
443	TCP	Jetty service (Jetty SSL port)	All servers and clients

Port	Type	Destination	Source
7001	TCP	Jetty service (Jetty alternate port)	Used for both site and base server
59100	TCP	Upload Controller service	All servers and clients
59108	TCP	Jetty service	AudioCodes Telephony Signaling port, MEDIA API

External Communication

Port	Type	Destination	Source
135 to 139 and 445	TCP	Storage Location	Jetty Service (File Transfer)

Media Encoder Component

The following table lists the ports on the Media Encoder server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
59109	TCP	Media Encoder service	All servers

External Communication

Port	Type	Destination	Source
135 to 139 and 445	TCP	Storage Location	Jetty Service (File Transfer)

Reconciliation Component

The following table list the ports for the Reconciliation service that must be opened in the Windows Firewall.

Inbound Ports

None

External Communication (* indicates default port)

Port	Type	Destination	Source
8443, 443, or 80	TCP	Unified CM Publisher and Subscribers	Reconciliation
1433*	TCP	SQL	Reconciliation
1504	TCP	Unified CCX Informix database	Reconciliation for Unified CCX

Desktop Client, Citrix Server, or Windows Terminal Services Component

The following table lists ports that must be opened in the Windows Firewall on the desktop client, Citrix server for thin client users, or Windows Terminal Services if you want to use the Live Screen Monitoring feature.

Inbound Ports

Port	Type	Destination	Source
49152 to 65535	TCP	Thin Client Screen Recording service	Live Screen Monitoring Client

Planning Ahead

Quality Management works with a variety of operating systems, software, and Automatic Call Distributors (ACDs). Deployment planning is required to ensure that the installation goes smoothly.

Use the information provided in the following topics to prepare for Quality Management deployment and installation activities.

Pre-Installation Checklists

Use the following pre-installation checklists to gather configuration information and prepare the servers before you install Quality Management.

Preparing a Site for Installing Quality Management Checklist

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

1. Complete the QM Site Configuration worksheet for your environment.

   This worksheet allows you to determine storage requirements for the primary recording storage location and the Recording Server temporary storage location (optional).

   This worksheet is available through the Cisco Implementation Services Help Desk.

2. Validate the Quality Management server hardware and capacity requirements for the following servers:

   - Base server
   - Recording Server
   - Monitor server

   See *System Requirements* and *System Requirements* for more information on hardware requirements.

3. Order the server hardware.

4. Install the Microsoft Windows Server operating system on the Quality Management server. For Microsoft Windows Server 2008 R2 and 2012:

   - Update to the latest service pack (SP)
   - Verify IIS or Web Services are not enabled (using port 80 or 443)
   - Install the Telnet client—Optional component for troubleshooting.

See Microsoft Windows Servers for more information on Microsoft Windows Server 2008 R2 or 2012.

5. Create the user accounts. You will need the following user accounts:

   - Local administrator account for installation on the server.
   - User account to connect to the external storage location—optional. This is only required for Site servers. The requirements for this account are as follows:
     - Local administrator
     - Set permission to run services

6. Install the Microsoft SQL Server. When installing the Microsoft SQL Server:

   - Verify Collation is SQL_Latin1_General_CP1_CI_AS
   - Verify Mixed Mode Authentication
   - Create an SQL Authentication User with the role of DBCreator

   See *Microsoft SQL Server* for information on settings.

7. Verify all required ports are open to the servers. See the *Quality Management Port Usage* for more information.
8. Verify the Quality Management software and license files are copied to the Quality Management base server.
9. Download the latest Quality Management Service Release (SR) and the latest Engineering Special (ES) from the Cisco website.
10. Load the Quality Management License on the Cisco Unified CCX server.
11. Review the *Release Notes*.

Cisco Unified CM Configuration Checklist

Use the following checklist to configure Cisco Unified CM.

1. Associate phones with the JTAPI user. See *JTAPI User* for more information.
2. Use the Cisco documentation to configure Network Recording or Network Based Recording (optional).

   - Create a recording profile
   - Create a SIP trunk

- Create a route pattern
- Assign the recording profile to the DN's to be recorded
- Configure DN for a monitoring calling search space
- Confirm the DN’s monitoring calling search space includes a route pattern

See *Configuring Cisco Unified CM Administration* for more information.

Cisco Unified CCX Configuration Checklist

Use the following checklist to configure Cisco Unified CCX.

Gamification Checklist

Use the following checklist to gather configuration information for the gamification feature before you install Quality Management.

> **Note:** Quality metrics are configured by default. No additional information is required.

1. Provide the IP address or hostname for the WFM server container.
2. Provide the port number for the WFM server container.

Deployment Checklists

Use the following deployment checklists when installing Quality Management and running the System Configuration Setup (postinstall.exe).

Single Server Installation Checklist

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

1. Install the required components on the Base server. See *Install Services on a Single Server* for more information.
2. Install the latest SR or ES, if available. See *Installing Quality Management* for more information on installing an SR or ES.
3. Complete System Setup Configuration (PostInstall)

   Use the information entered in the Use the information entered in the QM Express Site Configuration worksheet. See *Configuring Quality Management* for more information.
4. Update the digital certificate. See *Managing Certificates* for more information.
5. Install any additional servers (optional). This could include one or more of the following

servers:

- Backup CTI server
- Additional Cisco Unified CM Cluster CTI server
- Recording server
- Monitor server (Server Recording only)
- Monitor server and Recording Server

Quality Management Administrator Configuration Checklist

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

1. Configure the users.
    - Link ACD accounts (AD Authentication) or configure ACD accounts (QM Authentication)
    - Create Quality Management users
    - Assign roles
    - License users
2. (AQM licenses only) Configure the evaluation form worksheets.
3. Complete the Business Users Worksheet for each workflow. This worksheet is available through the Cisco Implementation Services Help Desk.
4. (AQM licenses only) Configure evaluation forms.
5. Configure the workflows.
6. (Required for Cisco MediaSense Recording, Server Recording, Network Recording, and Network Based Recording) Configure the VoIP devices.
    - Enable devices for recording
    - Set recording type
    - Assign agents to devices or configure devices for Hot Desking
    - Assign a Recording Server

- (Server Recording only) Assign a Monitor server

7. Configure the export settings.

Desktop Application Installation Checklist

Use the following checklist when installing Quality Management desktop applications.

1. (Citrix environment only) Install the Recording Thin Client on Citrix servers. See *Installing Server Applications* for more information on installing the Recording Thin Client.
2. Install Quality Management Administrator on select workstations. See *Deploying Applications on the Desktop* for more information.
3. Install the Desktop Recording service on all PCs that require audio recording or screen recording. See *Deploying Applications on the Desktop* for more information.
4. Install the latest SR or ES on the desktop, if available. See *Installing a Patch* for more information.

Optional Features Configuration Checklist

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

1. Configure the Inclusion List. See *Inclusion List* for more information.
2. Configure your custom metadata. See “User-Defined Metadata” in the *Administrator Guide*.
3. Configure the silence and talk over events. See “Call Events Administration” in the *Administrator Guide*.
4. Configure the MANA CDR. See *Monitoring and Notification* for more information.

   Note: This option is not required for Cisco MediaSense Recording.

5. (Required for Hot Desking if you are using Network Recording, Network Based Recording, Cisco MediaSense Recording, or Server Recording) Configure Hot Desking.
   a. Create a default Hot Desking agent. See the *Administrator Guide* for instructions.
   b. Install Recording Controls on the base server. See the *Developer, API, and Database Schema Guide* for instructions.

Testing Checklist

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

1. Play back an audio recording. See "Playing Recordings" in the *User Guide*.
2. Play back a screen recording (AQM or AQMS+). See "Playing Recordings" in the *User Guide*.
3. Play back a customer conversation. See "Playing Recordings" in the *User Guide*.
4. Monitor an active call using the Live Monitoring application. See "Live Monitoring" in the *User Guide*.

   Note: Live Monitoring is only available if you are using Network Recording.

5. Run a report. See "Reporting" in the *User Guide*.
6. Export a recording. See "Export Selected Contact" in the *User Guide*.

Before Installing Quality Management

Before you deploy Quality Management, you need to prepare the environment. The following topics describes how to configure the environment to support Quality Management.

Important: If you use the N or KN versions of Microsoft Windows, you must install the appropriate version of the Windows Media Feature Pack prior to installing . Determine the version of Microsoft Windows you are using by viewing System Properties (hold the Windows key and press Pause).

To locate the Windows Media Feature Pack, go to www.microsoft.com and search for “Media Feature Pack.” Download and install the Media Feature Pack for your version of your operating system.

Cisco Environment

If your site includes Cisco Agent Desktop and you want to use the Recording Monitoring application, you must select the following check boxes on the Agent Distribution tab in PG Explorer:

- Enable agent reporting
- Agent event detail
- Agent real time data
- Agent historical data

Install Cisco Unified CM per the Cisco documentation. Follow these guidelines when installing 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 postinstall.exe
  - Finding devices on the VoIP Devices window in Quality Management Administrator
- See the following topics for additional information:
  - *Configuring Cisco Unified CM Administration*
  - *JTAPI User*

Configuring Cisco Unified CM Administration

The following instructions explain how to configure Cisco Unified CM Administrator for Network Recording and Network Based 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 Setup” in the *Cisco Unified Communications Manager Administration Guide*. **Note:** BIB is required to use the silent monitoring and whisper features in the Live Monitoring application.
Step 2	Add a user for the monitoring and recording application.	See “Application User Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 3	Add the user to a access control group that allows monitoring and recording.	See “Application User Setup” and “Access Control Group Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 4	*Optional:* 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 Parameter Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 5	Configure DN for a monitoring calling search space.	See “Directory Number Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 6	Enable recording for a line appearance.	See “Directory Number Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 7	Create a recording profile.	See “Recording Profile Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 8	*Optional:* Create a SIP profile for Recording CTI service.	See “SIP Profile Setup” in the *Cisco Unified Communications Manager Administration Guide*.

Steps	Configuration Steps	Related Procedures and Topics
step 9	Disable the Timer Keep Alive Expires setting.	See “SIP Profile Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 10	Create a SIP trunk that points to the Recording CTI service.	See “Trunk Setup” in the *Cisco Unified Communications Manager Administration Guide*. **Note:** If you are using Network Based Recording, you must select the This trunk connects to a recording-enabled gateway check box.
Step 11	Create a route pattern for the Recording CTI service.	See “Route Pattern Setup” in the *Cisco Unified Communications Manager Administration Guide*.
Step 12	Configure the recorder for redundancy.	See “Trunk Setup” in the *Cisco Unified Communications Manager Administration Guide*.

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 and CUBE SIP 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 Gateway Recording or 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.

  Example: Unified CCX and Cisco Agent Desktop can share the same JTAPI user.

- 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.

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 Unified Workforce Optimization Container.
- Cisco only supports the US English locale on the server's operating system. Both the server and the server's local system user must use the US English locale.
- If a web service is installed on the server, make sure it does not use TCP ports 80, 443, or 7001. These ports are used by the Jetty service. See *Quality Management Jetty Component* for more information.

Microsoft SQL Server

Before you install the Quality Management, you must install Microsoft SQL either co-resident with the Web 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:

- 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.

Consult the SQL Server documentation for instructions on creating a login and password to connect to the SQL server. Quality Management will use the login and password to connect with the SQL server. You can specify more than one login and password.

> **Example:** You can configure one user login responsible for installation and upgrades and another user login responsible for day-to-day database activities.

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.

Note: Sort the Quality Management SQL Server login name and password in a save place. You will need this information for when you configure Quality Management.

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.

Example: Running backups three times a week.

See the Microsoft SQL Server documentation for instructions on creating a maintenance plan.

SQL Server Browser

The SQL Server Browser, a component in Microsoft SQL Server 2008 and Microsoft SQL Server 2012, 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.

> **Note:** 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. See Adding Firewall Exclusions by Program for more information.

Windows SNMP Service

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 postinstall.exe.) Install SNMP on the Web Base server running either Windows Server 2008 R2, Windows Server 2012, Windows Server 2014, or VMware ESX Server.

The SNMP Service requires that you ensure:

- The logged in user has Administrator privilege or is part of the Administrators group
- The network policies do not prevent installing new Windows services

For more information on installing and configuring this tool, see the Microsoft SNMP documentation and *SNMP Integration*.

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, in a single instance across one or more domains.

Example: Security policies like complexity level or duration.

If your system uses Active Directory, postinstall.exe prompts you to provide domain information for Active Directory.

When a user logs into Unified 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.

Note: The user configured for connecting to Active Directory must have `Read:Group Membership` permission enabled.

Active Directory Configuration Guidelines

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

- 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 postinstall.exe. See "Active Directory" in the *Administrator Guide* 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 can be assigned the system administrator role.
- User records—for recorded users (agents) and users who will log into Quality Management Administrator and Unified Workforce Optimization as an administrator.

Using OpenLDAP with Active Directory

You can use LDAP (Lightweight Directory Access Protocol) to query for user authorization against the customer's AD domain controllers, and you can use the LDAP proxy server to query multiple AD servers.

OpenLDAP uses a similar directory structure to that of Active Directory. The following table lists the srearch strings to use for searching for objects, users, and groups in OpenLDAP:

UserSearches	
Primary search object	`(objectClass=posixAccount)`
Specific user search	`(&(objectClass=posixAccount)(cn=<user_name>))`
Specific user last name search	`(&(objectClass=posixAccount)(sr=<last_name>))`
Specific first name search	`(&(objectClass=posixAccount)(givenName=<first_name>))`
Group Searches	
Primary Search object	`(objectClass=posixGroup)`
QM Admin Group Searching	For QM, the user is added to the Person table; information about the person needs to be added to OpenLDAP: ■ Search by specific name: `(&(objectClasss=posixGroup)(cn=<name_of_group>))` ■ When finding users of this group, search for the attribute `memberUid`, then search for the user with `(&(objectClass=posixAccount)(cn=<user_name>))`
WFM Admin Group Searching	For WFM, the only information needed is the user in the group: `(ObjectClass=posixGroup)(cn=<name_of_group>)(memberUid=<user_name>))`

External Storage User

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 postinstall.exe.

The Jetty service requires the external storage user to access the external storage location.

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*.

Zeranoe FFmpeg

Before you install Quality Management, you must download the 64-bit static FFmpeg.exe from http://ffmpeg.zeranoe.com/builds/. See *Install Services on a Single Server* for installation requirements.

> **Note:** In Quality Management versions prior to 11.5, the FFmpeg.exe file was downloaded to the C:\\Program Files\Cisco\WFO_QM\bin folder. If you uninstall Quality Management, you also uninstall FFmpeg. With these versions, if you uninstall and reinstall Quality Management, you must also reinstall FFmpeg.
>
> Beginning with version 11.5, the FFmpeg.exe file is downloaded to the C:\Program Files\Common Files\QM\bin folder. In this location, the file is not uninstalled when you uninstall Quality Management; as a result, you will not have to reinstall FFmpeg.exe.

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 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:
    - Web Base server (Jetty service)
    - Operations server (Upload Controller service)
    - Recording Servers
    - Site Upload server (Upload Controller service, Jetty service, and Media webapp)
- The administrator needs to connect to the Web 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

1. From the Web Base server, choose one of the following options:
    - Windows Server 2008:
        a. Choose Start > Settings > Control Panel.
        b. Double-click Regional and Language. The Regional and Language window appears.

    c. Click the Keyboards and Languages tab.

    d. Click the Install/Uninstall Languages button.

    e. Select the Install Display Languages and browse to the language pack, and then follow the prompts to install the fonts.

- For Windows Server 2012:

    a. Choose Desktop > Control Panel > Clock, Language, and Regions > Language. The Language window appears.

    b. Click Add a Language, select a language, and then click Add.

2. Restart the Web Base server. The server might automatically restart after you install the fonts.

3. Open Windows Explorer and go to C:\Windows\Fonts. The Fonts window appears.

4. Select and copy the font you just added.

    - Batang (Russian and Korean)
    - MingLiU (Chinese and Japanese)
    - A Unicode supported font (for example, Calibri)

5. Go to the C:\Program Files\Cisco\WFO_QM\Java\lib\fonts folder and choose Edit > Paste.

6. 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 reports using the PDF format, you must perform the following steps.

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

1. On the Web Base server, go to the ...\Program Files\Cisco\WFO_QM\Jetty\Cisco-solutions\reports folder and open the properties file associated with your locale.

    Example: Open QMReport_zh_CN.properties if your locale is Chinese.

2. Find encoding= and change it to encoding=UTF-8.

3. Find font=Arial and change Arial to one of the following font names:

- Batang (Russian and Korean)
- MingLiU (Chinese and Japanese)
- A Unicode supported font (for example, Calibri)

> **Note:** The font name must match the font name that appears in the Font name field when you double-click a font in the C:\Windows\Fonts directory.

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

   The Fonts window appears.

5. Select and copy the font you just added to the properties file.
   - Batang (Russian and Korean)
   - MingLiU (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.

Installing Quality Management

When you install Quality Management 11.5, you must choose one of the options in the following table and install the components as described.

To:	Do This:
Install a single server configuration	1. On the server, complete the steps in *Install Services on a Single Server*. **Important:** When you run System Configuration Setup on the Base server, configure all off-board servers. 2. Install the desktop applications. See *Deploying Applications on the Desktop*. 3. Update the digital certificate for the Base server. See *Managing Certificates*.

Services for Quality Management

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

Important: Install Web Base Services first in a multiple server configuration. You can install the remaining services on the other servers in any order you wish.

System Configuration Setup (postinstall.exe) runs automatically after you have installed a services on a server. When using postinstall.exe, you must complete postinstall.exe after an installation or an upgrade in order for the system to function.

Install Services on a Single Server

To install services on a single server:

1. Copy the setup_MonRec_<version>.exe, where <version> is the version number, to the Quality Management server.
2. Double-click the file setup_MonRec_<version>.exe to start the installation wizard.

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

3. Click Next to display the Select Destination dialog box.
4. The default path is C:\Program Files\Cisco. If you want to change the default folder, click Change and follow the prompts.

> **Note:** If you choose to change the path, do not specify the root directory (for example, D:\ or E:\). Always one folder level must be defined (for example, D:\Cisco\).

5. Click Next to display the Select Components window.
6. To install Quality Management on a single server, select Single Server from the Select Components drop-down list.

   The following services will be installed by default:

   - Web Base Services
   - Operational Base Services
   - Signaling Services > CTI Service

     > **Note:** You must select at least one signaling service.

   - Recording Services
   - Site Upload Services
   - Database Services
   - Encoding Services
   - Reconciliation Services
   - Monitoring Services

   > **Note:** You need to install all services that appear in this dialog box on the server.

7. To choose an additional service, select the check box for that service.
8. Click Next, and then click Install.

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 terminate when finished.

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

9. Select Launch product configuration to automatically launch System Configuration Setup (postinstall.exe).

   If you clear the Launch product configuration check box, postinstall.exe will NOT launch automatically when the installation is complete.

10. Click Finish to complete the installation of services.

    > **Note:** You might be prompted to reboot the machine to complete the installation. If you choose not to reboot now, changes will not go into effect until the machine has been rebooted.

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

11. Complete the System Configuration Setup. See *System Configuration Setup* for more information.
12. Download 64-bit static FFmpeg from the following website:

    http://ffmpeg.zeranoe.com/builds/

13. Extract the ffmpeg.exe from the bin folder in the zip file.
14. Install the ffmpeg.exe in the following folder on the Quality Management server:

    C:\Program Files\Common Files\QM\bin

Installing a Patch

Quality Management is upgraded periodically. The upgrade can be one of three types: an engineering test (ET), and engineering special (ES), or a service release (SR).

Engineering Test	ET is an additional installable component that contains the files needed to assist developers in diagnosing a problem. ETs are intended for limited scope tests.

Engineering Special	An ES is a version of the product that contains all fixes issued since the base release to the latest ES. Installing an ES replaces the existing installation.
Service Release	An SR is a version of the product that contains all fixes issued since the base release to the latest SR. Installing an SR replaces the existing installation.

Before you install a Quality Management ET, ES, or SR, do the following:

- Schedule the installation for a maintenance period when your Quality Management system is out of production.
- Back up the SQL Server for Quality Management database using SQL Server backup tools.
- Uninstall any existing ET.

All patches are installed over the top of the existing installation. For instructions, see *Installing an Upgrade*.

Running a Repair

You can use the Repair function in the Windows Programs and Features utility in Control Panel to correct problems that might arise.

To repair Quality Management:

1. Log into Quality Management as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.

   There can be up to three programs listed for Quality Management, depending on what you installed on the server:

   a. Cisco Monitoring and Recording Services Framework

   b. Cisco Monitoring and Recording Services

   c. Cisco Monitoring and Recording Services Jetty

   The repair function is only available for (b) or (c).

   Note: If you are not sure where the problem lies, run a repair on both programs.

3. Select the Jetty program and run a repair on it first.

4. Select the Services program and run a repair on it.
5. When the repairs are complete, start postinstall.exe.
6. Complete postinstall.exe, providing any information that might not be present. The repair function removes any changes that were made to the Windows Registry so you will have to enter some data to reconnect your Quality Management installation to the Quality Management database.

> **Note:** If there was an ET installed before you repaired Quality Management, you must reinstall it after the repair is complete.

Installing an Upgrade

Before You Begin

1. Request an upgrade plan from Cisco PDI.
2. Review the server hardware and scalability requirements. Your previous version of Quality Management might have different requirements than Quality Management 11.5. See *System Requirements* and *System Requirements* for more information.
3. Review the *Release Notes* and *Administrator Guide* for this release.
4. If you are upgrading from a version prior to 11.0 and you are using screen recordings, use the Cisco Screen Converter utility to upgrade your recordings before you install version 11.5. See *Cisco Screen Converter Utility* for instructions on how upgrade screen recording from the REC format to the M4V format.

Important: Screen recordings in REC format are not automatically upgraded to M4V format when you upgrade to 11.5. You must use the Cisco Screen Converter utility to upgrade your recordings before you install version 11.5.

Cisco Screen Converter Utility

Quality Management does not automatically upgrade REC format screen recordings to M4V format when you upgrade to version 11.5. Cisco provides the Cisco Screen Converter utility to allow you to upgrade your screen recordings to the M4V format. The Screen Converter utility supports upgrading screen recordings from version 10.0, 10.5, and 11.0.

You must install and run the Screen Converter (setup_MonRec_ScreenConverter.exe) utility on either a Site Upload server or a Media Encoding server. The Screen Converter utility requires Windows Server Desktop Experience to be installed and enabled. This utility is only available in an SR or ES for versions 10.0, 10.5, or 11.0. You might need to upgrade to the latest SR or ES that contains this utility.

The REC to M4V Encoder (RecToM4VEncoder.exe) converts the screen recordings in REC format in a specified storage directory to M4V format. The files are converted one by one starting with the most recent file.

Note that you can stop the RecToM4VEncoder.exe at any time. When you restart RecToM4VEncoder.exe, the conversion process starts again with the most recent file. You can also run RecToM4VEncoder.exe nightly on multiple conversion servers concurrently to more efficiently process a large number of REC files.

The approximate conversion time REC to M4V is 1:1 based on the total time of the REC screen recording.

Example: If the REC screen recording is three minutes, the time it takes to convert it to M4V is three minutes.

To install the Cisco Screen Converter Utility:

1. Go to the following directory on the Site Upload server or a Media Encoding server:

   C:\Program Files\Cisco\WFO_QM\Install

2. Double-click setup_MonRec_ScreenConverter.exe and follow the prompts.

To configure the RecToM4VEncoder.cfg:

1. Open the RecToM4VEncoder.cfg. The file is located at:

   C:\Program Files\Cisco\WFO_QM_ScreenConverter\config

2. Scroll to folderList= at the bottom of the file and enter the directory names that contain REC format screen recordings. Each folder name must be separated by "|".

   Example: folderList=C:\Program Files\Common Files\QM\Recording\Video|R:\MyRecordings

   Alternatively, you can include the directory names when you run RecToM4VEncoder from the command line using the following format:

   ```
   RecToM4VEncoder [-i <filename>|-f <foldername>] [-u]
   ```

   where <filename> is the path and file name of a specific REC file and <foldername> is the path to a specific directory that contains REC files, and -u displays this information screen.

   Example: RecToM4VEncoder -f C:\Program Files\Common Files\QM\Recording\Video

To run RecToM4VEncoder.exe:

1. From the command line, go the following directory:

   C:\Program Files\Cisco\WFO_QM_ScreenConverter\bin

2. To convert REC format screen recordings to M4V format, enter the following command:

```
RecToM4VEncoder
```

This command will convert the directories specified in RecToM4VEncoder.cfg.

Note: RecToM4VEncoder.exe does not support converting screen recordings that exceed 4096×4096 dimension. If a screen recording exceeds 4096×4096, the recording will not be converted to M4V.

Best Practices: Run the RecToM4VEncoder.exe before you upgraded to version 11.5. If you do not convert the screen recordings from REC to M4V format, "file not found" error will appear when you try to play back the recording in version 11.5.

Upgrading from a Previous Version

Quality Management supports direct upgrades from the following versions:

- Quality Management 10.5
- Quality Management 10.0
- Quality Management 9.0
- Quality Management 8.5(2)

Important: Over the top upgrades from version 10.5 and earlier to 11.5 are not supported. All such upgrades must be manual. This means that the old version of Quality Management (but not your Quality Management database) must be uninstalled before the new version is installed. Over the top upgrades from 11.0 to newer versions of 11.5 are supported.

If you are installing from a version prior to 10.0, upgrade to version10.0. Follow the upgrade instructions in the *CiscoRecording and Quality Management Installation Guide* for version 10.0.

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:

1. Choose one of the following options:

From Version	Instructions
earlier versions	1. Confirm you have the installation media and license for versions 10.0 and 11.5, including the latest Service Release (SR) and Engineering Special (ES). 2. Follow the upgrade instructions in the *Installation Guide* for version 10.0 and then uninstall 10.0.
10 or 10.5	Uninstall the existing Quality Management, and then install Quality Management. **Note:** Over-the-top installation is not supported.
11.0	Install Quality Management over-the-top (see *Upgrading Quality Management*).

2. Complete the steps in *Upgrading Quality Management*.

> **Important:** The system you are upgrading to must be running a 64-bit Windows Server. Upgrading from a 32-bit Windows Server is not supported.

3. Upgrade the desktop applications. See *Upgrading the Desktop Applications* for more information.

Evaluator Role

When upgrading from 11.0 or earlier, note that the evaluator permissions have changed. When you upgrade to 11.5:

- The All Managers Evaluate and All Supervisors Evaluate check boxes will be removed from the Evaluation Form Administration window
- User Administration window:
  - All existing evaluators will have their Evaluator Scope set to All Teams and the Auto Assign Evaluations check box will be cleared.
  - All other users will have their Evaluator Scope set to null and the Auto Assign Evaluations check box will be cleared

- If the All Managers Evaluate check box was selected in the Evaluation Form Administration window in the previous release then all managers will be assigned the evaluator role with Evaluator Scope set to Scope Additions
- If the All Supervisors Evaluate check box was selected in the Evaluation Form Administration window the previous release then all supervisors will be assigned the evaluator role with Evaluator Scope set to Scope Additions

CDR Configuration

When upgrading from 10.0(1), note that the CDR Configuration button moved to Unified CM under Telephony Groups in postinstall.exe and System Configuration.

Playing a Voice Recording

When upgrading from 10.0(1) or earlier, note that the behavior for downloading and playing a recording in the Media Player has changed.

For 10.0(1) and earlier, voice recordings were downloaded, unencrypted, and uncompressed when you played the recording in the Media Player. The voice recording was deleted when you changed focus from the Media Player to another application on Unified Workforce Optimization.

Starting with 10.5(1), voice recordings are downloaded, unencrypted, uncompressed, and streamed to your web browser when you play the recording in the Media Player. The voice recording is deleted when you clear the cache in your web browser.

> **Best practices:** Use HTTPS to connect to Unified Workforce Optimization through a web browser and configure the QM certificate. See *Managing Certificates* for instructions on generating certificates so that you can use HTTPS.
>
> In Microsoft Internet Explorer, select the Delete Browsing History on Exit check box on the General tab in the Internet Options dialog box. This ensures the cache, including all voice recordings, is cleared every time you exit Internet Explorer.

Recording Methods

When upgrading from 10.0(1), the “Recording Types” section was moved to the “Capture/Recording Methods (In-depth View)” section of the *Design Guide*.

Database Server

When upgrading from 11.0 or earlier, the Database Services bundle is no longer associated with the Database server and the Database Server option has been removed from the installer. The Database Services bundle is now associated with the Operations server.

If you are upgrading from a previous release that includes a Database server, when you run the installer on the Database server the selected component will appear as Custom installation.

Upgrading Quality Management

Use the following task to upgrade to 11.5.

1. On the SQL server, back up your Quality Management database. See *Quality Management Database Disaster Recovery* for instructions.

2. On the Web Base server, back up the Report Logo images—see *Custom Logo File Recovery* for instructions.

3. From the VoIP Devices window in Quality Management Administrator, export the VoIP devices as a CSV file. See "VoIP Devices" in the *Administrator Guide* for more information.

4. Install the latest Quality Management 11.5 (the version can include the latest SR or ES) on the web base server. See *Installing Quality Management* for instructions.

Upgrading Unified CM

Use the following task to updated to Quality Management after a Cisco Unified CM upgrade.

1. On the SQL server, back up your Quality Management database. See *Quality Management Database Disaster Recovery* for instructions.

2. On the Web Base server, back up the Report Logo images—see *Custom Logo File Recovery* for instructions.

3. Double-click PostInstall.exe manually on any Quality Management server. PostInstall.exe is located at:

   <install folder>\WFO_QM\bin\postinstall.exe

   where <install folder> is the path to postinstall.exe. The default path is C:\Program Files\Cisco\WFO_QM\bin\postinstall.exe.

4. Click OK to bypass the initial System Configuration Setup window.

5. From the VoIP Devices window in Quality Management Administrator, export the VoIP devices as a CSV file. See "VoIP Devices" in the *Administrator Guide* for more information.

6. Choose System Configuration > Telephony Groups and select a Unified CM telephony group.

   a. Select the current SOAP AXL version from the Version drop-down list.

   b. Click CDR Configuration and select the current Unified CM Version from the drop-down list.

c. Click OK, and then click Save.

7. On the server running the CTI service, select Tools > Download/Install JTAPI and follow the prompts.

> **Note:** If you are unsure where the CTI service is installed, go to the Status page on the Web Base serve and look at the list of Signaling Groups.

> **Important:** Do not manually install the JTAPI tools plugin from Unified CM. Installing the JTAPI from System Configuration Setup, ensures that additional functions are performed to establish support for JTAPI in a Quality Management environment.

This step must be performed on all servers running the CTI service.

The new JTAPI client will be installed and tested. If any errors appear, validate the Soap AXL configuration, JTAPI username and password, and try again.

System Configuration Setup

1. If System Configuration Setup does not launch automatically, you must launch it manually. To launch PostInstall manually on any Quality Management server double click:

   <install folder>\WFO_QM\bin\postinstall.exe

   where <install folder> is the path to postinstall.exe. The default path is C:\Program Files\Cisco\WFO_QM\bin\postinstall.exe.

2. Click OK to bypass the initial System Configuration Setup window.

3. Choose System Configuration > Telephony Groups and select a Unified CM telephony group.

   a. Select the current SOAP AXL version from the Version drop-down list.

   b. Click CDR Configuration and select the current Unified CM Version from the drop-down list.

   c. Click OK, and then click Save.

4. On the server running the CTI service, select Tools > Download/Install JTAPI and follow the prompts.

Note: If you are unsure where the CTI service is installed, go to the Status page on the Web Base serve and look at the list of Signaling Groups.

Important: Do not manually install the JTAPI tools plugin from Unified CM. Installing the JTAPI from System Configuration Setup, ensures that additional functions are performed to establish support for JTAPI in a Quality Management environment.

This step must be performed on all servers running the CTI service.

The new JTAPI client will be installed and tested. If any errors appear, validate the Soap AXL configuration, JTAPI username and password, and try again.

Configuring Quality Management

The System Configuration Setup (postinstall.exe) tool is used to configure Quality Management after you have installed Quality Management services.

Note: System Configuration Setup is generally referred to as "PostInstall" since its executable is postinstall.exe, and that is how it is referred to in this section.

Best Practice: The minimum network adapter internet speed should be at least 1 GBPS (full duplex).

PostInstall has two modes:

- **Initial Mode.** PostInstall is launched automatically in Initial Mode after the Quality Management installation (base, upgrade, and patches) finishes. After you configure all of the required parameters, the Quality Management services start automatically and the system is ready for use.
- **Update Mode.** Whenever you start PostInstall manually to change the configuration settings in an existing system, it starts in Update Mode. You start it manually to change the configuration settings in an existing system.

Note: PostInstall is present on every Quality Management server. It detects the services installed on that server and customizes the steps available accordingly. In a multiple server configuration, the instance of PostInstall that can change Quality Management settings is located on the web base server.

To launch PostInstall manually on any Quality Management server double click:

```
<install folder>\WFO_QM\bin\postinstall.exe
```

The default path is `C:\Program Files\Cisco\WFO_QM\bin\postinstall.exe`.

Postinstall.exe performs the following functions:

- Configures the system, including:
  - The location of the servers
  - The connection information for third party software

Example: You use postinstall.exe to configure the connection information for SQL, ACD, and 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

This section list of all possible windows or dialog boxes that can appear when you run postinstall.exe in Initial or Update Mode.

Note: Some steps trigger actions and do not display windows that contain fields to be completed.

System Configuration Setup

1. 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

   Best Practices: Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.

2. Enter the IP address or hostname of base server.

   The base server is the computer where you installed the Web Base Services, Database Services, Voice/Screen Services, and signaling service.

3. Enter the IP address or hostname of the Unified Workforce Optimization Container.

   The Unified Workforce Optimization Container is located on the base server.

   If you also purchased Workforce Management (WFM) and configured it to point to this container, it will share this container with Quality Management.

4. Choose the hostname or IP address for this server from the Local Services drop-down list, and then click OK.

Note: If you are configuring the Local Services on the web base server, this is the same hostname or IP address you entered in the Host Address for Base Server field.

Example: If you installed the Network Recording service and Monitor service on a different server, choose the Recording Server IP address 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.

5. (Initial Mode only) When the Installation Type dialog box appears, choose one of the following options and then click OK.

   - New Installation—choose this option if you are installing Quality Management in a new environment.
   - Upgrade—choose this option if you are upgrading Quality Management.

System Configuration Setup Tools

System Configuration Setup (postinstall.exe) 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 postinstall.exe, only enables tools when the tools are available on the server where you are running the postinstall.exe.

The following table displays the available tools and the servers on which they are located.

Tool availability in Postinstall

	Servers						
Tool	Web Base	Operations	Database	Site Upload	CTI	Voice Record & Monitor	Media Encoding
Start Local Services	x		x	x	x	x	x
Create Database Catalogs	x		x				
Generate Info for MSI Clients	x						

Tool	Servers						
	Web Base	Operations	Data base	Site Upload	CTI	Voice Record & Monitor	Media Encoding
Download/Install JTAPI					x		
Encrypt Audio Files				x			
Set Recording Home Directory				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	x
Choose Monitor Adaptor						x	
Remove Recording Services	x		x	x	x	x	x
Set Temporary Recording Directory						x	
Set Temporary Encoding Directory							x
SIP Trunk Certificate					x*	x	
Change IP Addresses or Host Names				x		x	x
Recording File Encryption Key							x

* When using secure SIP or SRTP, the CTI server requires a SIP Trunk Certificate.

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 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 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.

Generate SSL Certificate

This tool generates a security certificate for the Media webapp and Unified 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 Media webapp or Reports runs). This tool is available only when you run postinstall.exe on the Quality Management server (for reporting) and the Site Upload server (for Media webapp).

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 or CUBE SIP CTI service has the correct JTAPI and accepts connections. The tool makes a request to each running Recording CTI service or CUBE SIP 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 Unified Workforce Optimization.

Note: This tool is not required for Cisco MediaSense Recording.

If you made any changes to the Recording CTI service or CUBE SIP CTI service in postinstall.exe, you must restart the Recording CTI service or CUBE SIP 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 postinstall.exe, you must restart the 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 (postinstall.exe).

The monitor adapter dialog pops up automatically during postinstall.exe 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 Cisco 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, postinstall.exe moves the recordings to the new location.

Set Temporary Encoding Directory

This tool allows you to choose a temporary storage location for encodings before they are uploaded. You can change the temporary encoding location at any time. When you change the temporary encoding location, postinstall.exe moves the encodings 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 8.5 or later. See the Cisco CUCM documentation for any changes to the required CUCM configuration for your version.

> **Note:** This tool is not required for Cisco MediaSense Recording.

To manage a SIP trunk certificate:

1. Select Tools > SIP Trunk Certificate, choose one of the following options, and follow the prompts:
   - 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.
2. Copy and upload both the Certificate and Key files generated to any additional CTI servers using the same menu if you want every server to use the same certificate. Otherwise repeat this entire process for each CTI server.
3. Upload the Certificate file to your CUCM OS Administrator.

Change IP Addresses or Hostnames

This tool allows you to change the IP address or hostname for the Site Upload server (Site Services), Recording Server, Monitor server, and Media Encoding server (Encoding Server). During an upgrade, this feature runs automatically after the Quality Management Quality Management database is initialized.

Recording File Encryption Key

This tool enables you to generate and manage your own encryption keys if desired. It is available only on servers that host the Media Encoder Service. With it, you can generate a new key and export and import the keystore to and from a specified location.

About Encryption

Quality Management provides a set of default encryption keys. These default keys are global, not customer specific. They do not require backup because they can be restored when you reinstall the Site Upload Server bundle. Creating your own private encryption keys with the Recording File Encryption Key tool is optional.

IMPORTANT: If you decide to generate new encryption keys, you must generate them on only one Media Encoder Service server, and then import the keystore from that server to all other Media Encoder Service servers in your system. Do not generate keys on multiple Media Encoder Service servers.

Best Practice: It is strongly recommended that you export your keystore to a secure location for safekeeping. If you lose the keystore, you will not be able to read any of your encrypted files. The keystore cannot be recovered or regenerated.

Encrypting voice and screen recordings protects sensitive information such as Social Security numbers and credit card numbers. The encryption feature complies with the Payment Card Industry Data Security Standard (PCI DSS). When a recording is encrypted, the recording file stored on the agent’s computer or on the storage server cannot be copied and played back.

When you use the Recording File Encryption Key tool, you generate a new set of customer-specific keys. This provides a higher level of security for your contact center by ensuring that the encryption keys are unique. Recording file encryption uses an asymmetric key pair (public/private) to encrypt recording files. Once new keys are generated, the public key is published and all new recordings going forward are encrypted using the newly created public key. The private keys are used to decrypt the recordings for playback.

The Media Encoder service automatically detects new keys and uses these new keys within ten minutes of your generating the keys. The keys are stored locally on the Media Encoder service server under the Common Files folder. This ensures the keys are not modified or lost during an upgrade.

Recordings are placed in a queue for encryption after the recording ends. The time it takes to complete the encryption depends on the system’s volume and load. They are then uploaded through an encrypted connection to the storage server.

Managing Encryption Keys

To generate a new key, follow these steps:

1. On a Media Encoder Service server, choose Tools > Recording File Encryption Key > Generate New Key. A warning dialog box appears.
2. Read the warnings, and then click Yes to continue.

Note: If the warning tells you that this server does not have the latest keystore, it means that a new key was previously generated on a different Media Encoder Services server and that this server does not have that key, making it impossible for this server to decrypt recordings encrypted with the newer key. You should import the latest keys to this server before generating a new key on it.

3. The new key is generated and placed in the local keystore, located here:

   ```
   C:\Program Files\Common Files\QM\config\filecryptokeystore
   ```

WARNING: **Never** change the filecryptokeystore file in any way, delete it, or paste a changed version over the file. Doing so makes recording calls impossible.

Always use the PostInstall Recording File Encryption Key import/export options to export the filecryptokeystore file. Always remember to keep the file in a secure place.

Note: When upgrading from a previous version of QM that used Proxy screen recordings (such as version 9.3 and earlier), keep your filecryptokeystore file from the earlier version to use with the RecToM4VEncoder utility. This utility needs that file to decrypt the older screen recordings, and to re-encode them for playback in the new version.

To export a keystore, follow these steps:

1. On the Media Encoder Service server where you generate new keys, choose Tools > Recording File Encryption Key > Export Keys.
2. Browse to a location to save the keystore, such as a portable flash drive, or to a secure location for safekeeping.
3. Name the keystore, then click Okay to export the keystore. You cannot overwrite an existing exported keystore.

To import and merge new keys into the local keystore on another Media Encoder Service server, follow these steps:

1. On one of the Media Encoder Service servers in your system, choose Tools > Recording File Encryption Key > Import Keys.
2. Navigate to the location where you exported the keystore, select the keystore, and click Okay.
3. The new keys in the keystore are merged into the local keystore on this server, located at:

```
C:\Program Filesl\Common Filese\QM\config\filecryptokeystore
```

4. Repeat these steps on all Media Encoder Service servers in your system except the one from which the keystore was exported.
5. After the keystore is imported to all Media Encoder Service servers, restart all instances of the following services:
   - Desktop Recording Service
   - Network Recording Service (VoiceRecordServer.exe)
   - Recording Thin Clients (ScreenRecordServer.exe)

   The new key will not be used for encryption until these services are restarted.

Installation Type

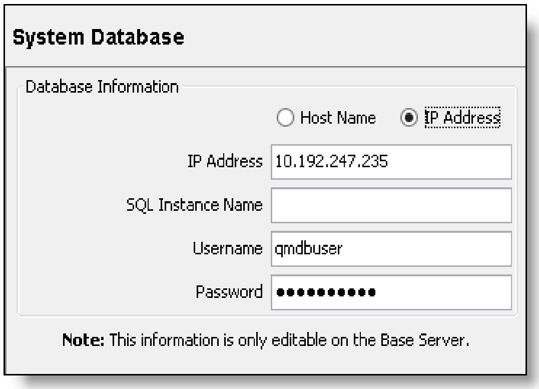
The Installation Type dialog box appears only during Initial Mode.

Choose the type of installation you want to perform. Your options are:

- New Installation—choose this option if you are installing Quality Management in a new environment.
- Upgrade—choose this option if you are upgrading Quality Management.

System Database

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



System Database

Database Information

○ Host Name ● IP Address

IP Address	10.192.247.235
SQL Instance Name	
Username	qmdbuser
Password	●●●●●●●●●●●

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

Note: You can only change the information in the System Database window from the postinstall.exe or Quality Management Administrator on the Web Base server. The System Database window in Quality Management Administrator on a desktop is read-only.

Field	Description
Host Name/IP Address	The hostname or IP address of the system operations server (the server on which SQL Server is installed). If you need to specify a configured port on the system operations server where an external SQL server will listen, choose Host Name and use the following format in the IP Address field: <IP address or hostname>:<port number> where <IP address or hostname> is the IP address or hostname and <port number> is the configured port number of the system operations server. **Example:** 10.188.252.11:1455 **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
SQL Instance Name	The SQL instance name of the Microsoft SQL Server service. Leave this field blank if you want to use the default instance name. The default instance name is automatically assigned when Microsoft SQL Server is installed.
Username	The username used by the Quality Management's DB Proxy service, for example qmdbuser, to access the system database. This username must be assigned the db_datareader, db_datawriter, and db_owner roles. See *Microsoft SQL Server* for more information.
Password	The password used by the DB Proxy service to access the system database. See *Microsoft SQL Server* 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.

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.

Update IP Address or Hostname

When upgrading Quality Management, you will be prompted to update the IP addresses or hostnames for the servers.

To modify the IP address or hostname for a server:

1. Click Modify, complete the fields, and click OK.
2. Repeat step 1 for each additional server.
3. Click Continue with These Changes.

To continue without making any changes to the IP address or hostname:

- Click Continue without Making Changes.

Database Exists

If the Database Exists dialog box appears, click OK to upgrade your database.

The program upgrades the database and loads default data into the database.

Databases Loaded

If the Database Loaded dialog box appears, click OK to dismiss the Database Loaded dialog box.

This dialog box appears when the database loads successfully.

Choose Temporary Storage Location

If you want to change the path to the temporary storage location, click Open, navigate to the folder in which you want to temporarily store recordings, and click OK.

Note: The Choose Temporary Storage Location dialog box only appears if this is a new installation.

Choose Temporary Encoding Storage Location

Choose a directory where encoding files will be processed from the Directory drop-down list. The specified directory must be accessible by the Local System user.

Update IP Address or Hostname

If required, update the IP address or hostname for the following servers and then click Continue with These Changes:

- Site Upload server (Site Services),
- Recording Server
- Monitor server
- Media Encoding server (Encoding Server)

Note: This dialog only appears when you are upgrading from a previous version of Quality Management.

Best Practices: Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.

Data Synchronization

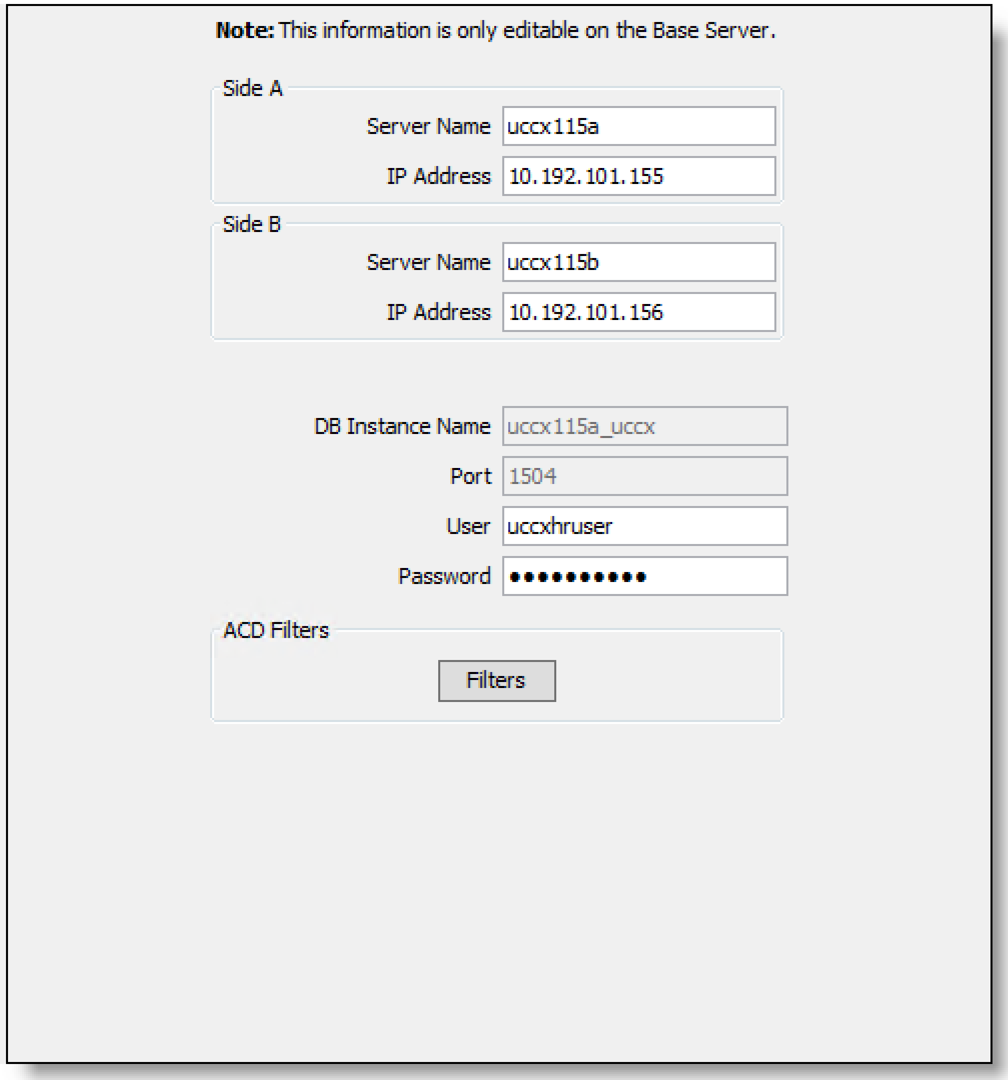
Use the Data Synchronization window to add, modify, or delete the connection information to Unified CCX.

Note: You can only change the information in the Data Synchronization window from the postinstall.exe or Quality Management Administrator on the Web Base server. The Database Synchronization window in Quality Management Administrator on a desktop is read-only.

You can configure the connection information to one or more Unified CCXs.

If you modify the information in the Data Synchronization window after the initial installation and configuration, you must restart the Sync services before your changes take effect.

The following window shows the configuration for a Unified CCX.



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

Side A

Server Name uccx115a

IP Address 10.192.101.155

Side B

Server Name uccx115b

IP Address 10.192.101.156

DB Instance Name uccx115a_uccx

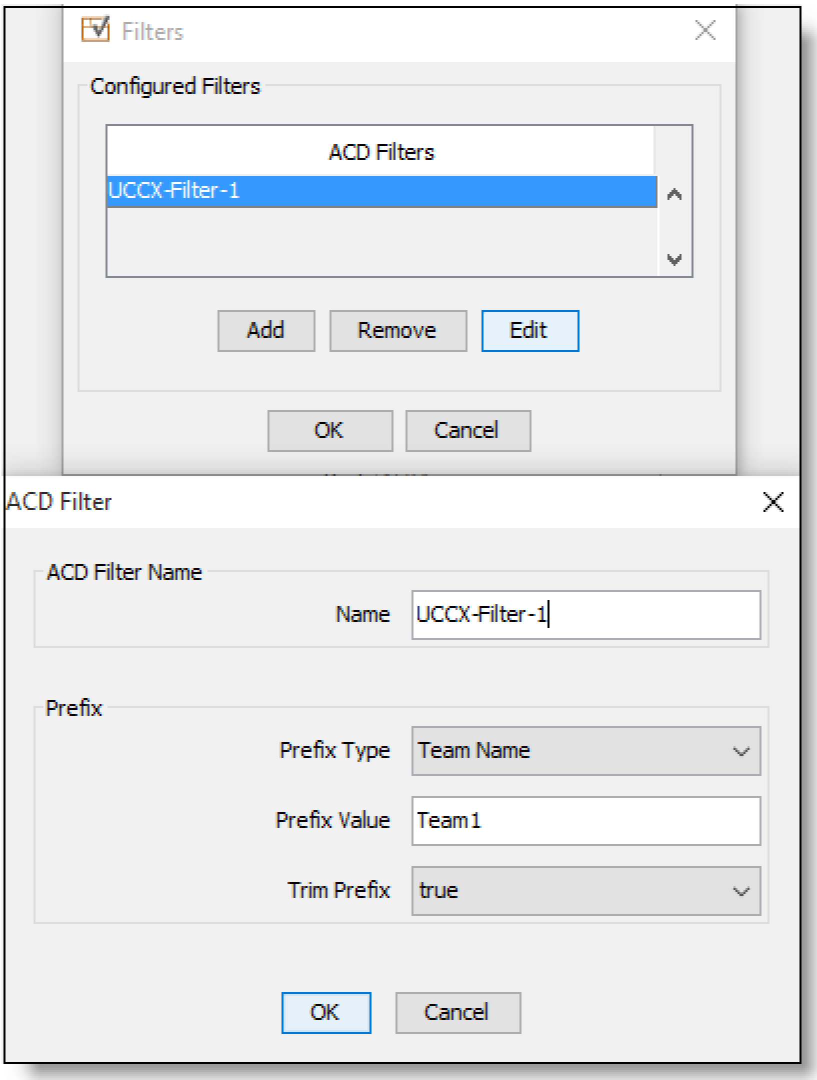
Port 1504

User uccxhruser

Password ●●●●●●●●●●

ACD Filters

The image below illustrates the Unified CCX filters:



ACD Filters

UCCX-Filter-1

Name: UCCX-Filter-1

Prefix Type: Team Name

Prefix Value: Team1

Trim Prefix: true

Field	Description
Add	Add an ACD.
Rename	Rename a selected ACD.
Delete	Delete a selected ACD. **Note:** When you delete an ACD, all associated data (that is, teams and users) will be deleted.
Unified CCX	

Field	Description
Side A Server Name	The name of the Unified CCX server for the Side A (primary) Cisco Unified CC database. **Note:** The server name must match the case of the name on the Unified CCX server. If the server name is all lowercase on the Unified CCX server, you must enter it as all lowercase in this field. If the server name contains a hyphen (-), replace the hyphen with an underscore (_). If the server name starts with a number, add the letter "i" to the beginning of the instance name. For example, if the server name is "100-voiceuccx-01", enter "i100_voiceuccx_01".
Side A IP Address	The IP address for the Unified CCX server for the Side A (primary) Cisco Unified CC database.
Side B Server Name	The name of the Unified CCX server for the Side B (secondary) redundant Cisco Unified CC database, if one exists. **Note:** The server name must match the case of the name on the Unified CCX server. If the server name is all lowercase on the Unified CCX server, you must enter it as all lowercase in this field. If the server name contains a hyphen (-), replace the hyphen with an underscore (_). If the server name starts with a number, add the letter "i" to the beginning of the instance name. For example, if the server name is "100-voiceuccx-01", enter "i100_voiceuccx_01".
Side B IP Address	The IP address for the Unified CCX server for the Side B (secondary) redundant Cisco Unified CC database, if one exists.
DB Instance Name	The name of the Cisco Unified CCX database. The name is <side A server name>_uccx and the field is disabled by default.
Port	The port number used by the Cisco Unified CCX database. The port number is 1504 and the field is disabled by default.

Field	Description
User	Login ID used to access the Cisco Unified CC database and synchronize users in a Unified CCX environment. This user must have read permission to the database. The login ID is uccxworkforce by default. **Note:** If you are using Cisco MediaSense, use uccxhruser for the login ID. This login ID has the permissions required to synchronize users and reconcile contacts. The uccxworkforce login ID does not have permission to use contactcalldetail and agentconnectiondetail tables that are required for reconciliation.
Password	Password used by uccxworkforce to access the Cisco Unified CC database in a Unified CCX environment.
ACD Filters	Allows you to determine what data is synced and determines which devices are available in a telephony implementation. See *Touch-Point Filtering* for more information.

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.

Service	Configuration settings applied when...
ACD Data Synchronization Service	Changes take effect immediately.
Reconciliation Service	Changes take effect immediately.

Service	Configuration settings applied when...
Sync Service	No restart is required: - After the initial installation - After you fix incorrect sync information The next sync period applies the configuration settings without restarting the Sync service. **Best Practices:** When there are substantial changes to the database, update the settings in the Cisco Unified CC Database in the following order: 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 third 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.

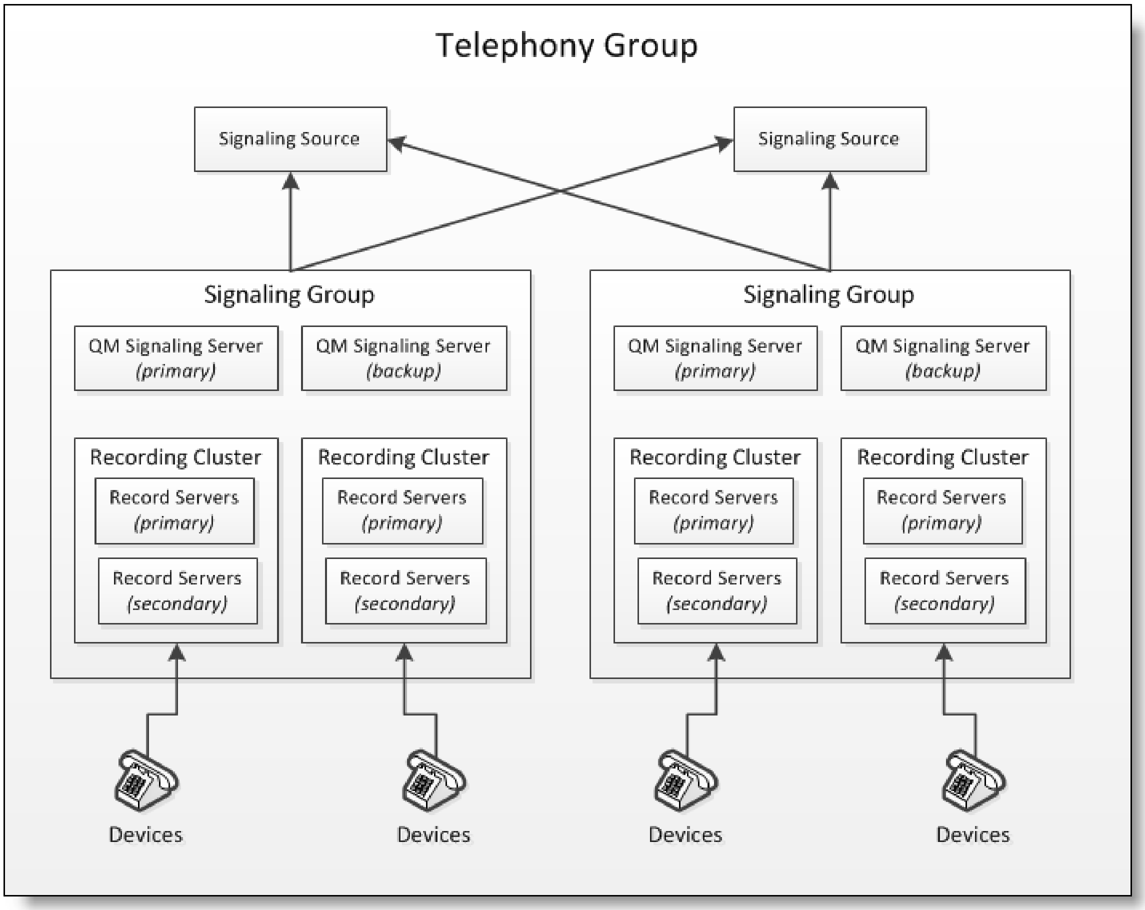
Field	Description
Name	The name of the ACD filter.
Prefix Type	The type of prefix that Touch-Point Filtering will use to filter the data. In this instance, the data is filtered by Team Name.
Prefix Value	The name of the team. No wildcards are allowed. **Example:** If you enter Team1, both Team1 and Team10 will be synced.
Trim Prefix	Remove the prefix before adding synced information to the Quality Management database. Your options are as follows: ■ True—removes the prefix. True is the default value. ■ False—keeps the prefix **Example:** QM_TeamA becomes TeamA.

Telephony Groups

A telephony group consists of at least one signaling source, one signaling group, one signaling server, one recording cluster, and devices.

Quality Management allows you to add backups for the signaling source, signaling group, signaling server, recording cluster, and devices. Adding any one of these backups is optional. However, Cisco recommends using backups for resiliency purposes.

Note: Some telephony group types do not support a backup signaling source.

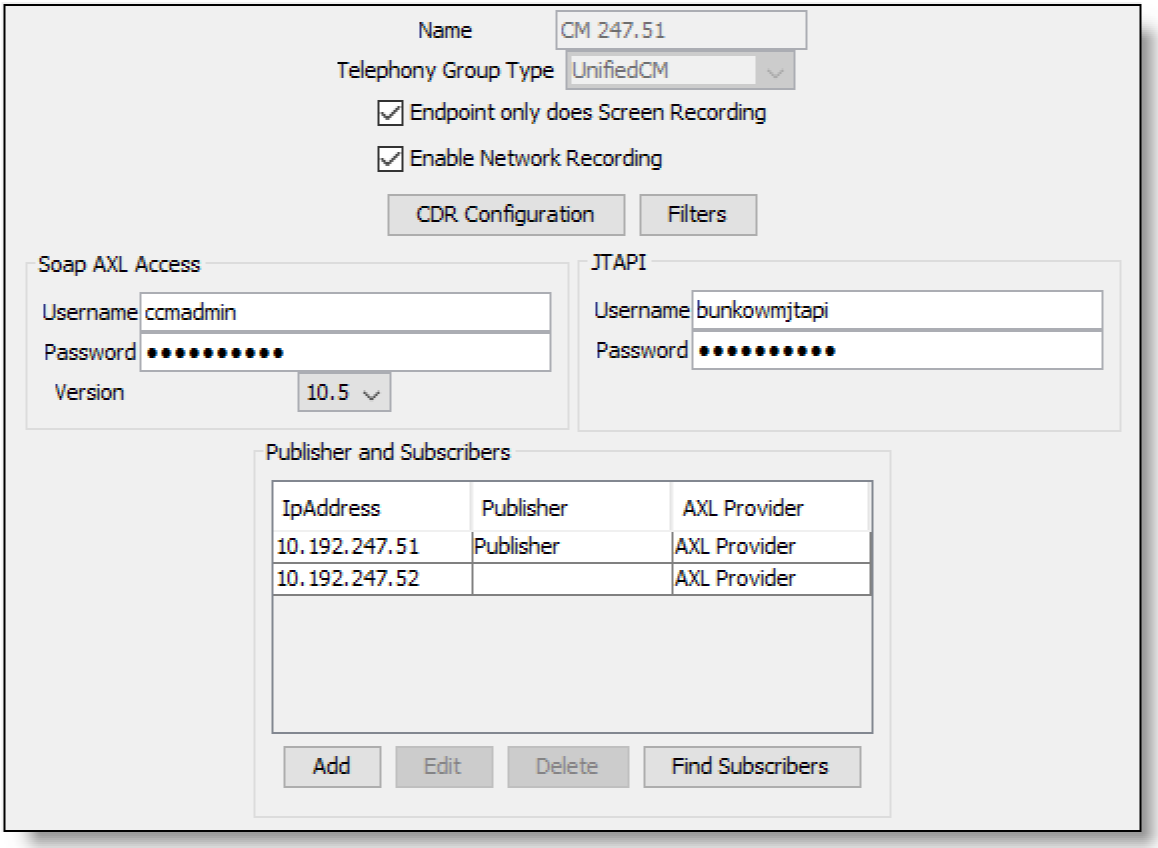


The Telephony Groups window allows you to add, modify, and delete the telephony groups:

Field	Description
Add	Add a telephony group and complete the following fields: ▪ Name—Enter a unique name for the telephony group. **Best Practices:** Specify a name that identifies how the telephony group is being used (for example, location, recording cluster, recording type, and so on). ▪ Telephony Group Type—Select the telephony group type from the drop-down list.
Rename	To change the name of the selected telephony group, enter the name in the New Name field and click OK.
Delete	Delete the selected telephony group. **Note:** If you delete a telephony group, Quality Management will remove all devices associated with this telephony group from the VoIP Devices table.
Revert Recent Changes	Reverts changes made after the last save to previously committed configuration settings.
Show Gateway Recordings Prior to Reconciliation	When selected, this check box allows archive users in an Unified CCX environment to view root calls in the Recordings application before the calls are reconciled, including all PCI events. When cleared, calls do not appear in the Recordings application until reconciliation is complete and all PCI events are excluded. This check box is clear by default.

Telephony Groups

The following window shows the Cisco Unified Call Manager Telephony Groups screen:



Name: CM 247.51

Telephony Group Type: UnifiedCM

☑ Endpoint only does Screen Recording

☑ Enable Network Recording

Soap AXL Access

Username: ccmadmin

Password: ●●●●●●●●●●

Version: 10.5

JTAPI

Username: bunkowmjtapi

Password: ●●●●●●●●●●

Publisher and Subscribers

IpAddress	Publisher	AXL Provider
10.192.247.51	Publisher	AXL Provider
10.192.247.52		AXL Provider

The following table describes what is supported based on telephony group type.

Telephony Group Type	Changes
Unified CM	A Unified CM telephony group can have any number of signaling groups.
All Others	All other telephony group types can support multiple telephony groups, but they are restricted to a single signaling group and Recording Cluster per telephony group.

Signaling Groups

Signaling groups are unique to the selected telephony.

A Unified CCX signaling group consists of one or more signaling services. Each CTI service in a Unified CM signaling group can have a separately administered list of Unified CM CTI Managers to connect to for JTAPI. The signaling group can have any number of Recording Clusters.

All other telephony group types are restricted to a single signaling group and Recording Cluster per telephony group. CUBE supports primary and backup signaling services, but MediaSense supports only a single signaling service.

Recording Clusters

Quality Management supports Recording Clusters. A Recording Cluster is a group of one or more Recording Servers. A Recording Server indicates which Recording Cluster it belongs to when it connects to a signaling service.

You can assign a Recording Servers to a Recording Cluster. When configuring a Recording Cluster remember the following points:

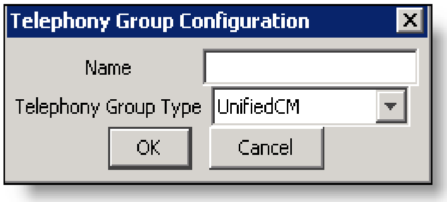
- If you have knowledge workers in a CUBE or MediaSense Recording environment who require screen recording, you need to create a Recording Cluster that connects to a CTI server and has no Recording Servers assigned to it.
- You can assign one or more Recording Servers to a Recording Cluster. A Recording Cluster requires at least one primary Recording Server.

  A primary signaling service will exhaust the capacity of all primary Recording Servers before sending calls to secondary Recording Servers. A backup signaling service will exhaust the capacity of all secondary Recording Servers before sending calls to primary Recording Servers. This allows primary/backup signaling services and primary/secondary Recording Servers to be split geographically while keeping the traffic as local as possible. Significant traffic should only traverse the WAN in specific failure scenarios.
- A Recording Server can only belong to one Recording Cluster.
- You can move Recording Servers between Recording Clusters.

Important: You must run postinstall.exe on all Recording Servers before you can assign a Recording Server to a Recording Cluster. If you do not run postinstall.exe on the Recording Servers the Select Record Servers dialog box will be empty.

Telephony Group Configuration

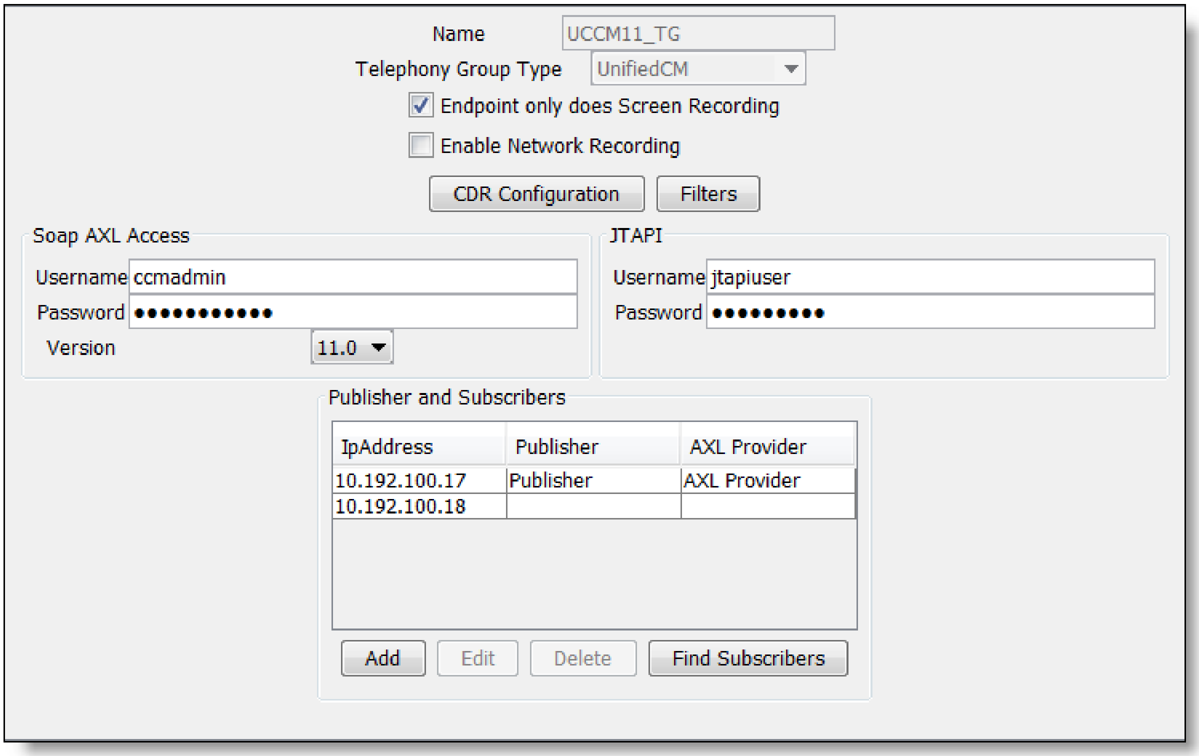
The Telephony Group Configuration dialog box appears when you add a telephony group. It allows you to assign a name to the telephony group and associate it with a telephony signaling method.



Field	Description
Name	The name of the telephony group. The name must be unique.
Telephony Group Type	The telephony signaling method for Unified CM. The possible telephony group types are as follows: ▪ CUBE—no additional configuration is required after you add this telephony group. ▪ Unified CM—see Unified CM Configuration for more information. The field displays Unified CM by default. ▪ MediaSense—see *MediaSense Configuration* for more information.

Unified CM Configuration

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



Name UCCM11_TG

Telephony Group Type UnifiedCM

☑ Endpoint only does Screen Recording

☐ Enable Network Recording

Soap AXL Access

Username ccmadmin

Password ●●●●●●●●●●●

Version 11.0

JTAPI

Username jtapiuser

Password ●●●●●●●●●

Publisher and Subscribers

IpAddress	Publisher	AXL Provider
10.192.100.17	Publisher	AXL Provider
10.192.100.18		

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 comprises a set of Unified CM servers that share the same database and resources and 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. For more information on CTI Managers, see *Signaling Groups*.

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 postinstall.exe 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.

Field	Description
Name	(Read only) The name of the telephony group. The name must be unique.
Telephony Group Type	(Read only) Displays Unified CM 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. The Desktop Recording service will not record audio when this box is selected. This only applies when you are using one of the following recording methods: ▪ Network Recording ▪ Cisco CUBE Recording via SIP Recording ▪ Cisco 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. You can install the Recording CTI service and CUBE SIP CTI service on the same machine if you clear the Enable Network Recording check box. **Example:** You are recording voice through Gateway Recording (using the CUBE SIP CTI service) and recording screen from a single server. **Note:** The Recording CTI service and CUBE SIP CTI service will interfere with each other while listening for SIP messages if the Enable Network Recording check box is selected.
CDR Configuration	Allows you to enable the Unified CM’s Call Detail Records (CDR) Report. See *CDR Configuration* for more information.

Field	Description
Filters	Allows you to configure the telephony filters for this telephony group. See *Filters* for more information. Use a telephony filter to filter the devices that are imported.
SOAP AXL Access Username	The AXL (Administrative XML Layer) authentication username on the publisher 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. **Note:** If you change a username or password, you must restart all associated signaling services.
SOAP AXL Access Password	The AXL authentication password on the publisher. This password is created when you configure Unified CM. **Note:** You must type this password; you cannot use copy/paste to enter the Unified CM password.
SOAP AXL Access Version	The Unified CM version on the publisher. **Note:** An error message will appear if the Version field is not configured.
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. **Note:** If you change a username or password, you must restart all associated signaling services.

Field	Description
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. **Note:** You must type this password; you cannot use copy/paste to enter the Unified CM password.
IP Address	The host name or IP address of the subscriber (if any) Unified CMs. You can enter one 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.
Publisher	The field indicates whether or not the provided Host Name/IP address is associated with the publisher CTI Manager service. If the field is blank, the Host Name/IP address is associated with a subscriber CTI Manager service.
AXL Provider	This field indicates whether or not the provided Host Name/IP address is associated with the AXL provider.
Add	Add a new publisher or subscriber. See *Subscriber Configuration* 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 credentials and to populate the list of subscribers, if any are found.

CDR Information Formats for the QM3002 Notification Trigger

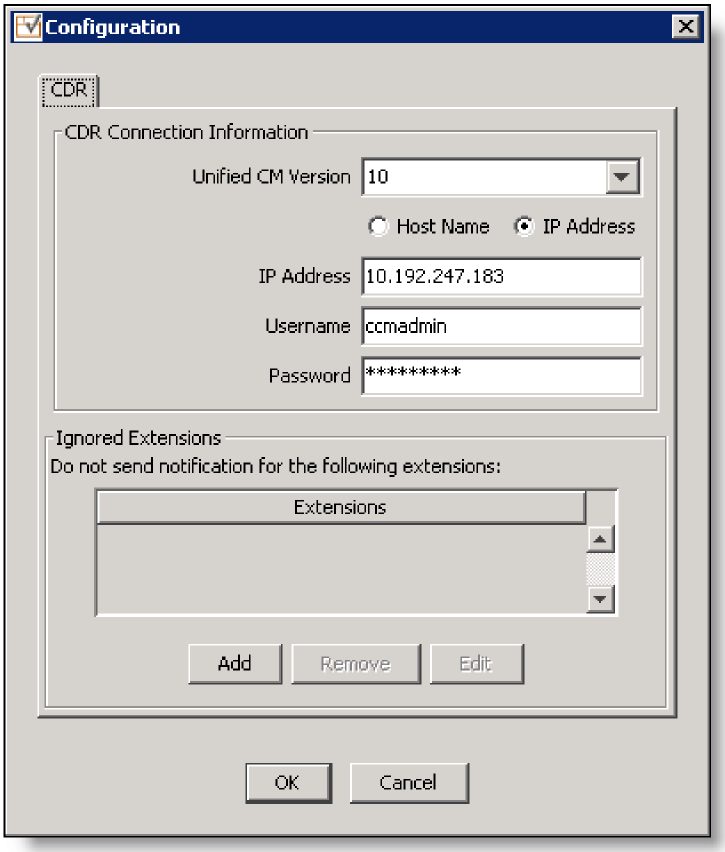
You can specify in which format you want to display the CDR information in the CDR Configuration dialog box. Examples of the available formats are listed here.

In these reports, call durations are expressed in milliseconds.

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

CDR Configuration

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


Configuration
CDR
CDR Connection Information
Ignored Extensions
Do not send notification for the following extensions:
Extensions
Add
Remove
Edit
OK
Cancel

Unified CM Version: 10
○ Host Name ● IP Address
IP Address: 10.192.247.183
Username: ccmadmin
Password: *********

Field	Description
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. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.

Field	Description
Username	The name of the user with rights to access the CAR reports. **Note:** If you change a username or password, you must restart all associated signaling services.
Password	The password of the user with rights to access the CAR reports.
Ignored Extensions	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. ■ Add—add a new extension to the list ■ Remove—delete an extension from the list ■ Edit—modify a selected extension in the list

Filters

Field	Description
Telephony Filters	Lists the names of the available telephony filters.
Add	Add a new telephony filter.
Remove	Delete a selected telephony filter.
Edit	Modify a selected telephony filter.
Name	The name of the telephony filter.
Extension Range	The range of device extensions that you want to include in the sync. An extension range comparison is done numerically. Pluses are limited from the numbers and compared mathematically. In this case, a range of 1 to 1000, would find the extension 500 in range.

Field	Description
Device Name Range	The range of device names that you want to include in the sync. Device names are compared alphabetically and/or lexicographically. So a range of 1 to 1000 would not find 500, instead you would have to specify the range as 0001 to 1000. This is because device names can be any string and are not limited to mostly being numbers as extension are.

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

Select a Unified CM telephony group from the list of telephony groups in the Telephony Groups window, click CDR Configuration, and choose one of the following options:

- To add an ignored extension, click Add in the Ignored Extensions section, enter the extension in the field, and click OK.
- To edit an ignored extension, select the extension from the Ignored Extensions list, click Edit, make the necessary changes in the Edit Extension dialog box, and click OK
- To remove an ignored extension, select an extension from the Ignored Extensions list and click Remove.

Configuring the QM3002 Notification Trigger

This task describes how to configure the QM3002 notification trigger.

1. Click CDR Configuration in the Unified CM Configuration window for a Unified CM telephony group type.

   The Configuration dialog box appears.

2. Select the version of the Cisco Unified CM you are using from the Unified CM 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.

   Enter the name and password of the user with rights to access the CAR reports.

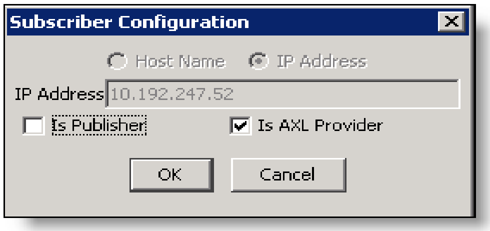
5. Add the extensions that you do not want to receive notifications. See Managing Ignored Extensions for more information.

6. Configure the properties for the notification.

7. Click OK.

Subscriber Configuration

Use the Subscriber Configuration dialog box to add a Unified CM server to the Cisco Unified CM cluster. Alternatively, you can use the Find Subscribers button in the Unified CM Configuration dialog box to find the list of subscribers.



○ Host Name ● IP Address

IP Address 10.192.247.52

□ Is Publisher ☑ Is AXL Provider

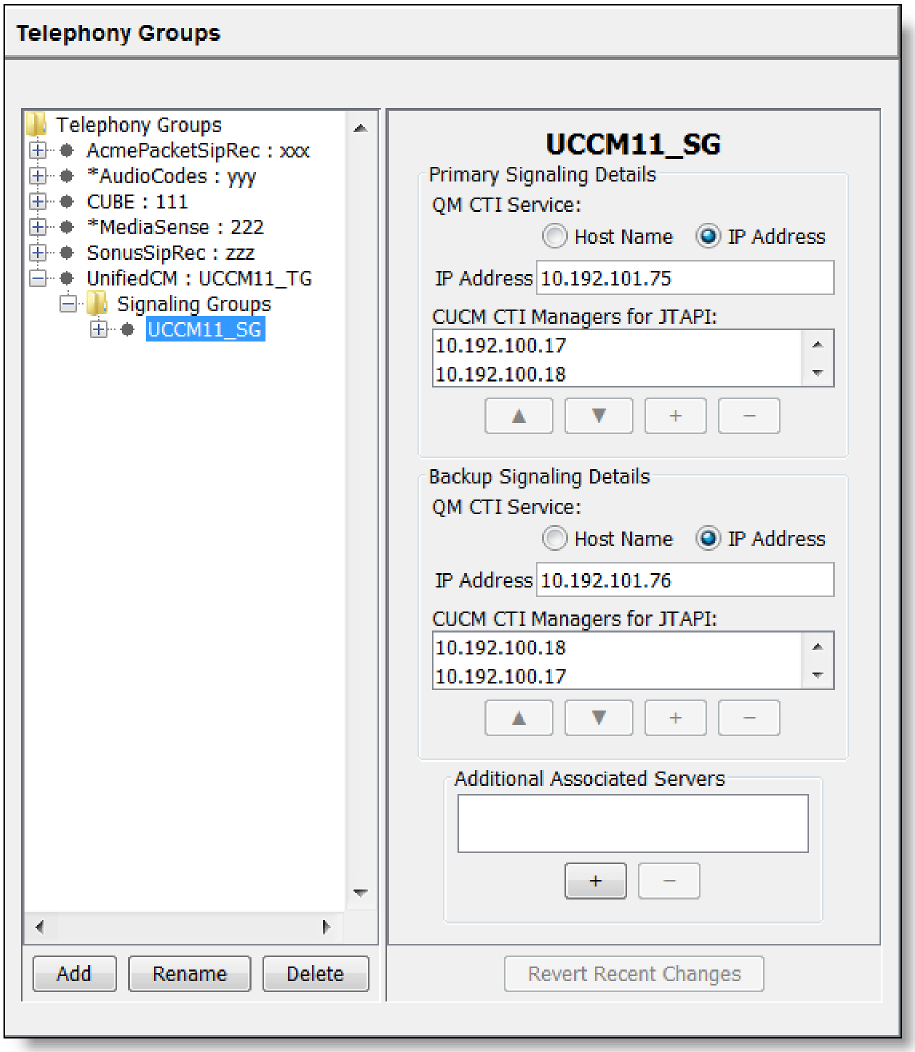
Field	Description
Host Name/IP Address	The host name or IP address of the publisher or subscriber (if any) Unified CMs. You can enter up to 8 subscriber Unified CMs. **Note:** When using hostnames, verify the server can resolve the name of the publisher or subscribers. If the hostname cannot be resolved, the Recording CTI service cannot log in. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
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.

Field	Description
Is AXL Provider	Select this check box if the provided Host Name/IP address is associated with the AXL provider.

Unified CM Signaling Group

For the Unified CM telephony group, 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.



Telephony Groups

- Telephony Groups
  - AcmePacketSipRec : xxx
  - *AudioCodes : yyy
  - CUBE : 111
  - *MediaSense : 222
  - SonusSipRec : zzz
  - UnifiedCM : UCCM11_TG
    - Signaling Groups
      - UCCM11_SG

UCCM11_SG

Primary Signaling Details

QM CTI Service: ○ Host Name ● IP Address

IP Address 10.192.101.75

CUCM CTI Managers for JTAPI:

10.192.100.17
10.192.100.18

Backup Signaling Details

QM CTI Service: ○ Host Name ● IP Address

IP Address 10.192.101.76

CUCM CTI Managers for JTAPI:

10.192.100.18
10.192.100.17

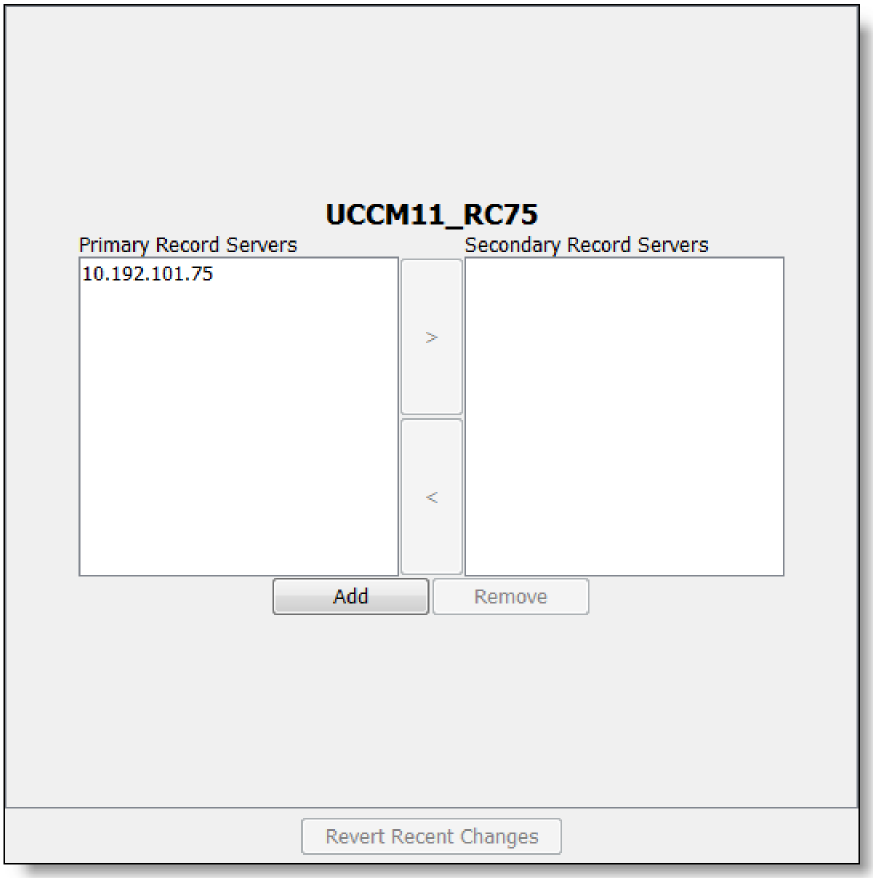
Additional Associated Servers

Field	Description
Primary Signaling Details	
Host Name/IP Address	The hostname or IP address of the primary signaling service. A primary hostname or IP address is required. This signaling service can belong to more than one signaling group. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
CUCM CTI Managers for JTAPI	The IP address of one or more primary CTI Managers. The CTI Manager is a service that runs on Unified CM and handles JTAPI events for every Unified CM in the cluster.
Backup Signaling Details	
Host Name/IP Address	The hostname or IP address of the backup signaling service. A backup hostname or IP address is optional. This signaling service can belong to more than one signaling group. **Note:** The signaling service remains on the backup server until you manually initiate fail back to the primary server. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
CUCM CTI Managers for JTAPI	The IP address of one or more backup CTI Managers. The CTI Manager is a service that runs on Unified CM and handles JTAPI events for every Unified CM in the cluster.
Additional Associated Servers	IP addresses for the remaining subscribers that are not associated with the primary and backup CUCM CTI Manager for JTAPI.

Field	Description
Up Arrow or Down Arrow	Use the Up or Down arrow buttons to move the CUCM CTI Managers to the desired location.
Add	Allows you to add a CUCM CTI Manager.
Delete	Allows you to delete a selected CUCM CTI Manager.

Unified CM Recording Cluster

Configure a recording cluster for Unified CM.



UCCM11_RC75

Primary Record Servers: 10.192.101.75

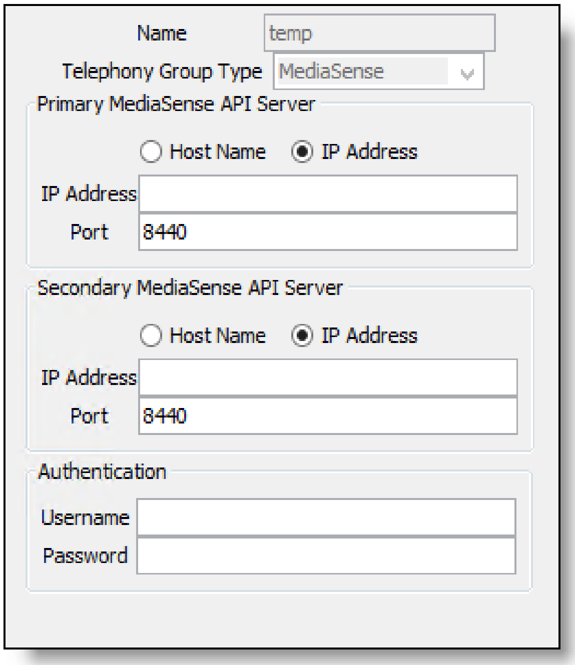
Secondary Record Servers:

Field	Description
Primary Record Servers	The primary Recording server assigned to this recording cluster.

Field	Description
Secondary Record Servers	The secondary Recording server assigned to this recording cluster.
Left Arrow or Right Arrow	Use the left or right arrow buttons to move the selected Recording Server to the desired location.
Add	Allows you to add one or more Recording Server as primary or secondary Recording servers.
Remove	Allows you to delete a selected Recording Server.

MediaSense Configuration

The MediaSense Configuration dialog box 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.



Name: temp

Telephony Group Type: MediaSense

Primary MediaSense API Server

○ Host Name ● IP Address

IP Address:

Port: 8440

Secondary MediaSense API Server

○ Host Name ● IP Address

IP Address:

Port: 8440

Authentication

Username:

Password:

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.

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. **Best Practices:** Use a hostname for the primary and secondary MediaSense API server, if possible.
Secondary MediaSense API Server IP Address or Hostname	The hostname or IP address of the secondary Cisco MediaSense API server. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
MediaSense Subscription Service IP Address or Hostname	The hostname or IP address for the MediaSense Subscription service.
Authentication Username	The username for the Cisco MediaSense API server. **Note:** If you change a username or password, you must restart all associated signaling services.
Authentication Password	The password for the Cisco MediaSense API server.

MediaSense Signaling Group

There is no configuration required for the MediaSense signaling group.

MediaSense Recording Cluster

There is no configuration required for a MediaSense recording cluster.

Managing Telephony Groups

To add a telephony group:

1. From the Telephony Groups window, select the Telephony Groups node, click Add, complete the fields, and then click OK to create a telephony group.
2. If there are fields associated with the new telephony group, complete the fields.

   Note: You cannot continue to the next step until you complete the fields.

3. Expand the new telephony group node, click Signaling Groups, click Add, complete the field, and then click OK to create a signaling group.
4. Complete the fields for the signaling group.

   Note: You cannot continue to the next step until you complete the fields.

5. Expand the new signaling group node, click Recording Clusters, click Add, complete the field, and then click OK to create the new recording cluster.
6. Complete the fields for the Recording Cluster and then click Save.

Configuration Settings Used By Services

If you change the settings for a telephony group, the following table shows when your changes take effect.

Telephony Group Type	Service	Configuration settings applied when...
CUBE	CUBE SIP CTI Service	Restart the service.
MediaSense	Monitoring and Recording MediaSense Subscription service	Restart the service.

Telephony Group Type	Service	Configuration settings applied when...
Unified CM	Recording CTI Service	Restart the service.
	Quality Management Administrator (VoIP Devices)	Reload the VoIP Device window.
	Desktop Recording service	Restart the service.
	Network Recording service	Restart the service. **Note:** If you add a backup Recording CTI Service from the postinstall.exe while in Update Mode, you must restart the Network Recording service.

Active Directory Options

Choose one of the following options from the Active Directory Options drop-down list.

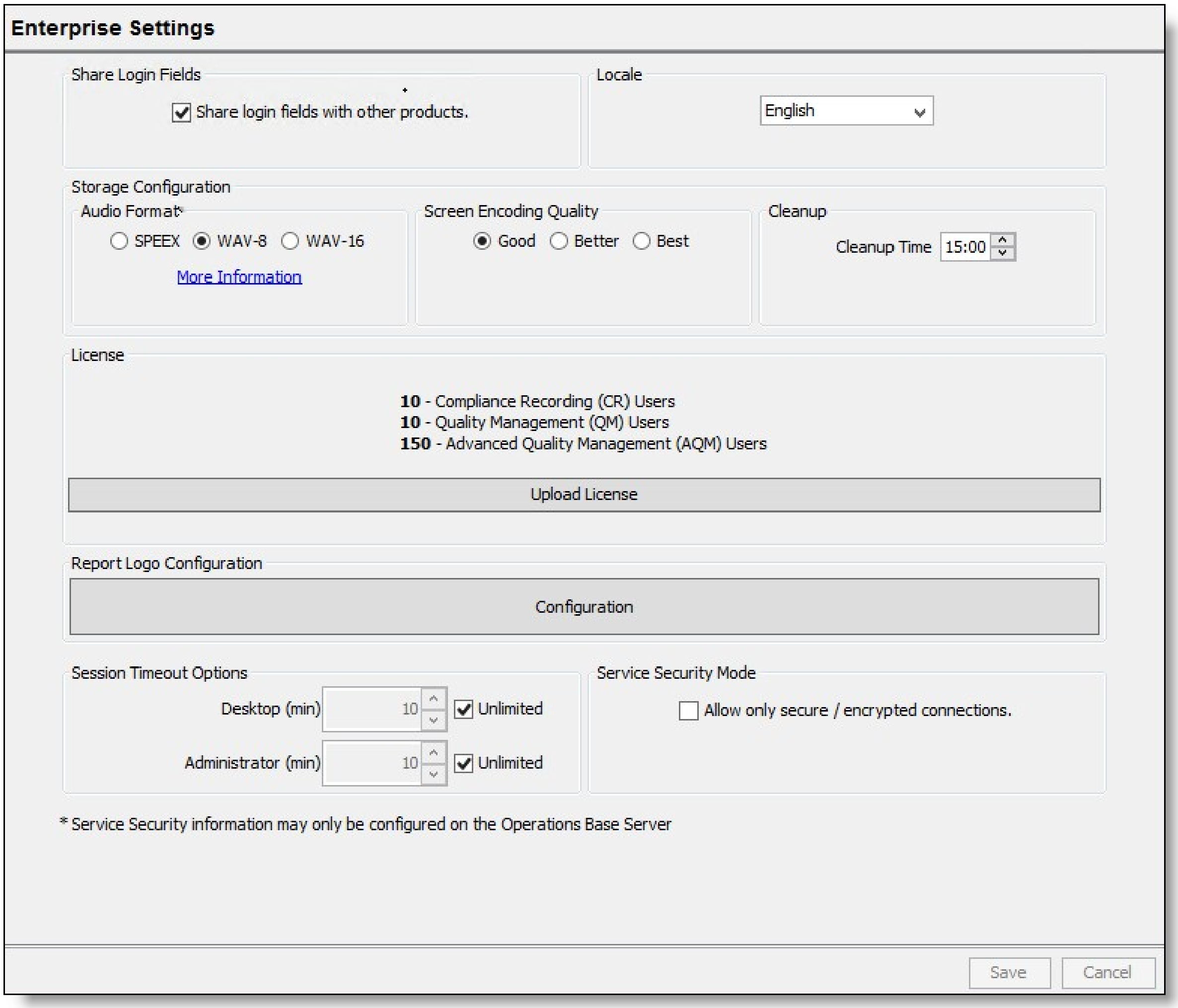
- Use Active Directory—Choose this option if you want to use Active Directory to authenticate user names and passwords.
- Use QM Authentication—Choose this option if you want to use Quality Management to authenticate user names and passwords.

JTAPI Completed Successfully

Click OK to dismiss the confirmation box.

Enterprise Settings

Use the Enterprise Settings window configure the settings for Quality Management.



Enterprise Settings

Share Login Fields

☑ Share login fields with other products.

Locale: English

Storage Configuration

Audio Format*: ○ SPEEX ● WAV-8 ○ WAV-16

More Information

Screen Encoding Quality: ● Good ○ Better ○ Best

Cleanup

Cleanup Time 15:00

License

10 - Compliance Recording (CR) Users
10 - Quality Management (QM) Users
150 - Advanced Quality Management (AQM) Users

Report Logo Configuration

Session Timeout Options

Desktop (min) 10 ☑ Unlimited

Administrator (min) 10 ☑ Unlimited

Service Security Mode

□ Allow only secure / encrypted connections.

* Service Security information may only be configured on the Operations Base Server

The Enterprise Settings window allows you to:

- Share login fields with other products. See the following topics for more information:
  - *Sharing Unified Workforce Optimization with Multiple Products*
  - *Share Login Fields*
- Configure the locale for your system if your version of Quality Management supports other languages in addition to English. See *Configuring Quality Management* for more information.
- Choose the default audio format for your recordings.

- Select the quality of your screen recordings:

Quality Level	Encoding Bit Rate	Screen Speed	Screen CPUs
Good	200	1 (real-time)	0 (1 code)
Better	400	2 (better)	1 ((cores/2)-1)
Best	600	2 (better)	2 (cores-1)

The higher the quality level selected , the more system resources are used.

- Specify when the DB Cleaner service runs.
- View license information and update software licenses, if you are not using an ACD, by importing a new software license file. See *Configuring Quality Management* for more information.
- Configure the report logo that appears in reports generated in the Reporting application. See *Report Logo Configuration* for more information.

> **Note:** The Report Logo Configuration button is only enabled from postinstall.exe or Quality Management Administrator on the Web Base server.

- Configure session timeouts for Recording and Quality Management and Quality Management Administrator. See *Session Timeout Options* for more information.
- Configure the security mode to allow only secure and encrypted connections. See *Service Security Mode* for more information.

Sharing Unified Workforce Optimization with Multiple Products

Unified 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 postinstall.exe.

> **Best Practice:** If you are using multiple Unified Workforce Optimization products, you should configure your Jetty web server to use 1024 MB of RAM for each product.

Share Login Fields

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

- Quality Management
- 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.

Best Practices: Select the Shared Login Fields check box.

If a user is not configured for multiple Cisco products or the user wants to log into both of the Cisco 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 Cisco product.

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

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

Locale

Use the Locale section to enable the default language in the Unified Workforce Optimization interface. Users can change the default language when they log in to Unified Workforce Optimization.

Note: The Locale section only appears when multiple locales are available.

To change the default locale for the Unified Workforce Optimization interface:

- Select the desired language from the Locale drop-down list.

Storage Configuration

Use Storage Configuration to manage the storage of recordings, including: the default audio format and the database cleanup time.

Choose the default audio format. Your options are as follows:

- SPEEX—provides the smallest file size. Choose this option if your greatest concern is to maximize storage space. When upgrading from 10.0 or lower, the default is SPEEX.
- WAV-8—files are approximately four times larger than SPEEX files. Choose this option if you want to compromise between greater audio fidelity and storage space.

- WAV-16—files are approximately twelve times larger than SPEEX files. Choose this option if you want the maximum audio fidelity and you are not concerned with storage space.

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: 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.

License

This section displays the available licenses and allows you to import licenses. The license type determines what Quality Management records. When a user logs into Unified Workforce Optimization, that user has access to all Quality Management applications allowed by the license and roles assigned to that user. The license determines what is recorded, not what is viewed, in Unified Workforce Optimization.

Example: If Agents X and Y use AQM or AQMS+ license, they can record their screens. For more information on Licensing, see "Mixed Mode Licensing" in the *Design Guide*.

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 postinstall.exe, Quality Management will continue to try connecting to the CVD. You will not be able 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 CR license to the AQM license), 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).

Note: Beginning with QM 11.0, only the AQM and AQMS+ licenses are available. QM and QMA licenses are not available.

Contact your sales representative to obtain a new license file.

To import a Cisco CR license file:

1. Click the Upload License button.

   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.

   If you are fixing a corrupted license, upload your existing license file.

3. Click Upload File.

   The Licensing Server uploads the Cisco CR license file.

Report Logo Configuration

Report Logo Configuration allows you to customize the logo that appears in reports generated by the Reporting application in Unified Workforce Optimization.

Custom logos must conform to the following specifications:

- The logo must be 60 × 60 pixels
- It must be in PNG format
- The file must be named "logo.png"

To replace the default logo with your own custom logo:

1. Navigate to the `C:\Program Files\Cisco\WFO_QM\Jetty\report_solutions\reports folder`, copy the original logo.png and save it to a backup folder.
2. Copy and replace the custom logo.png to the following folders:
   - `C:\Program Files\Cisco\WFO_QM\Jetty\report_solutions\reports`
   - `C:\Program Files\Common Files\QM\config`

   Note: By copying your custom logo file into the Common Files folder, it will be available even if you upgrade to a new version. PostInstall automatically copies it from the Common Files folder to the correct folder within the Quality Management file structure every time it is run.

3. Start postinstall.exe or Quality Management Administrator.
4. On the Enterprise Settings window, click Report Logo Configuration.
5. Click Select New Logo, browse to the location of your logo, and then click Select Image.

6. Click Save.
7. Restart the Jetty service.

To restore the default logo:

1. On the Enterprise Settings window, click Report Logo Configuration.
2. Click Use Default Logo and then click Save.
3. Restart the Jetty service.

Session Timeout Options

You can configure Quality Management Administrator or Recording and Quality Management in Unified 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 timeout)
- 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 Recording and 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 customer conversation, the session remains in an active state. Unified Workforce Optimization does not time out when you are playing a customer conversation.

Service Security Mode

If you configured the servers to run with Secure Socket Layer (SSL) and plan to use Hypertext Transfer Protocol Secure (HTTPS), some traffic will continue through non-secure transport. Specifically, voice and screen uploads will continue over non-secure transport as the data is already encrypted.

Select the Allow secure / encrypted connections check box to enable secure (HTTPS) connections for traffic other than voice and screen upload. When this check box is selected, you must use HTTPS when connecting to Unified Workforce Optimization. Once enabled, you will not be allowed to play back recordings or live monitor a user if you are using HTTP to connect to Unified Workforce Optimization.

When the check box is selected, the useSSL flag for web, voice, and screen servers will be set to true and their httpPort setting will use the statically defined value of 7001.

Note: You will need to manually block port 80 if required. See the "Quality Management Port Usage" in the *Installation Guide* for more information on port usage.

When the check box is cleared, the useSSL flag for web, voice, and screen servers will be set to false, and their httpPort setting will use port 80.

Licenses Validated Successfully

Click OK to dismiss the License Validated Successfully 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.

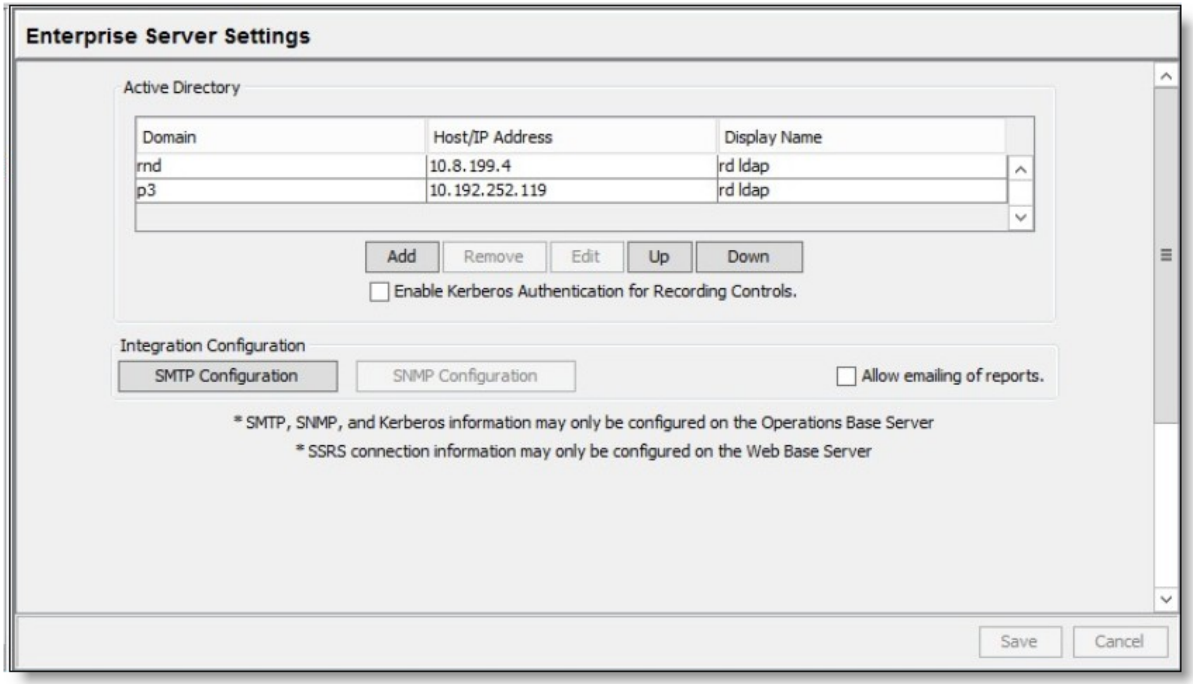
This password allows the administrator to access Quality Management Administrator and Unified Workforce Optimization. The password must be between 1 and 32 characters long. It is case sensitive.

Note: If you are installing Quality Management for the first time, the Old password field is disabled.

Pack noEnterprise Server Settings

Use the Enterprise Server Settings window to configure Active Directory. You can also configure the method (SMTP or SNMP) used to notify administrator or supervisors of system problems, and enable the ability to email reports.

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



Enterprise Server Settings

Active Directory

Domain	Host/IP Address	Display Name
rnd	10.8.199.4	rd ldap
p3	10.192.252.119	rd ldap

□ Enable Kerberos Authentication for Recording Controls.

Integration Configuration

□ Allow emailing of reports.

* SMTP, SNMP, and Kerberos information may only be configured on the Operations Base Server

* SSRS connection information may only be configured on the Web Base Server

The Enterprise Server Settings window allows you to:

- Configure Microsoft Active Directory domains (in an Active Directory system only). See *Active Directory* for more information.

- Enable Kerberos Authentication for Recording Controls. When enabled, a user must enter their AD credentials to access Recording controls. This check box is enabled only when Active Directory is enabled.

  > **Note:** You will be prompted to restart the Jetty service. Changes to Kerberos Authentication goes into effect after the Jetty service is restarted.

- Configure the method (SMTP or SNMP) used to notify administrators or supervisors of a system problem and decide if emailing reports will be allowed.

Configuration Settings Used By Services

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

Service	Configuration settings applied when...
Quality Management Administrator (AD Authentication and Administrator session timeout change)	Log into Quality Management Administrator.
Unified Workforce Optimization (AD Authentication and localization changes)	Start the Data API service.
Kerberos Authentication for Recording Controls	Restart the Jetty service

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.

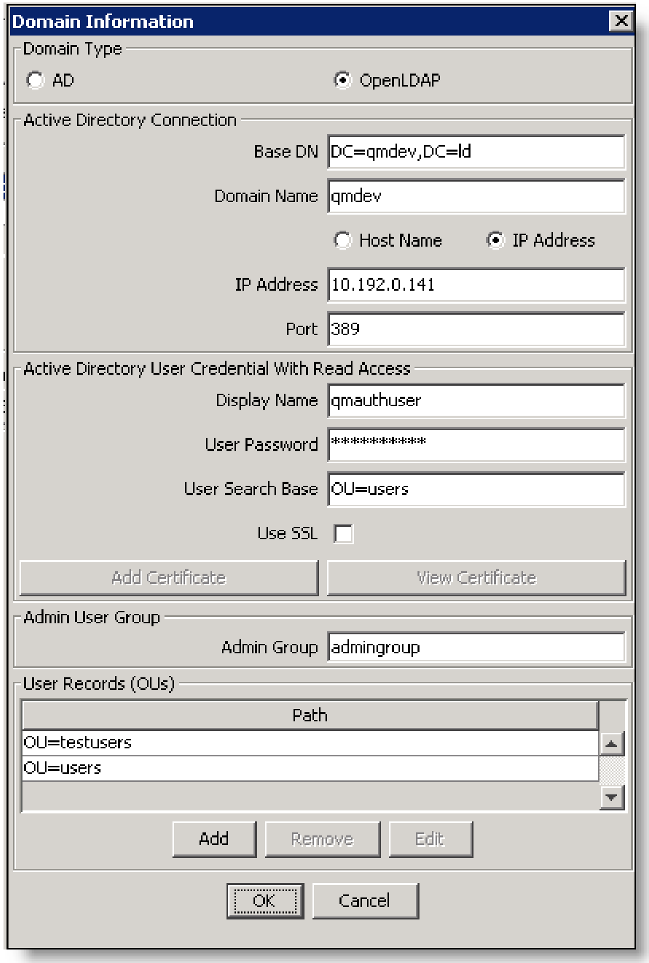
- There must be at least one domain configured
- Each domain must have at least one user path configured

To add or delete an Active Directory domain from the Enterprise Settings window:

- 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.

Domain Information

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



Domain Information

Domain Type
○ AD
● OpenLDAP

Active Directory Connection
Base DN DC=qmdev,DC=ld
Domain Name qmdev
○ Host Name ● IP Address
IP Address 10.192.0.141
Port 389

Active Directory User Credential With Read Access
Display Name qmauthuser
User Password ***********
User Search Base OU=users
Use SSL □

Admin User Group
Admin Group admingroup

User Records (OUs)

Path
OU=testusers
OU=users

Field	Description
Domain Type	Select the domain type: ■ Active Directory ■ OpenLDAP
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=*domain* statements to the beginning of the Base DN field.

Field	Description
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.
Host Name/IP Address	The host name or IP address of the Active Directory server. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
Port	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). **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. The Quality Management server must allow socket communication on this port to be able to access the Active Directory server for user authentication.
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.

Field	Description
Admin Group	The name of the security group in Active Directory. Only users assigned to this security group can be assigned the system administrator role. **Note:** All users in the Admin Group must belong to the same domain specified in the Base DN field. **Note:** AD Account users associated with the Security Group setting are not given an administrator role by default. To assign the system administrator role to a user in this security group, see *Administrator Configuration*. **Best practice:** Create a security group with a unique name in Active Directory and add the users who you want to have system administrator privileges in Quality Management Administrator and Unified Workforce Optimization. Specify the name of that security group in this field. This prevents any conflict with default security groups in Active Directory. Note that adding users to the Domain Admins group is not appropriate in this instance because the users in the Domain Admins group also have permission to make changes in Active Directory.

Field	Description
Add Certificate	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. 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: `http://<Active Directory server IP address or hostname>/<certsrv>` You can use certificate enrollment tools other than certsrv in this command. **Note:** Quality Management can only import Distinguished Encoding Rules (DER) encoded binary X.509 or Base-64 encoded X.509 formatted certificates. These files typically have one of the following extensions: der, pem, or cer. 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. **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.
View Certificate	View the certificate associated with Active Directory.

Field	Description

User Records (OUs)	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.
	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:
	`ou=US`
	`    ou=Minnesota`
	`        ou=Minneapolis`
	`            ou=Users`
	Then the user record appears as follows:
	`ou=Users,ou=Minneapolis,ou=Minnesota,ou=US`
	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.
	`ou=Minnesota,ou=US`

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

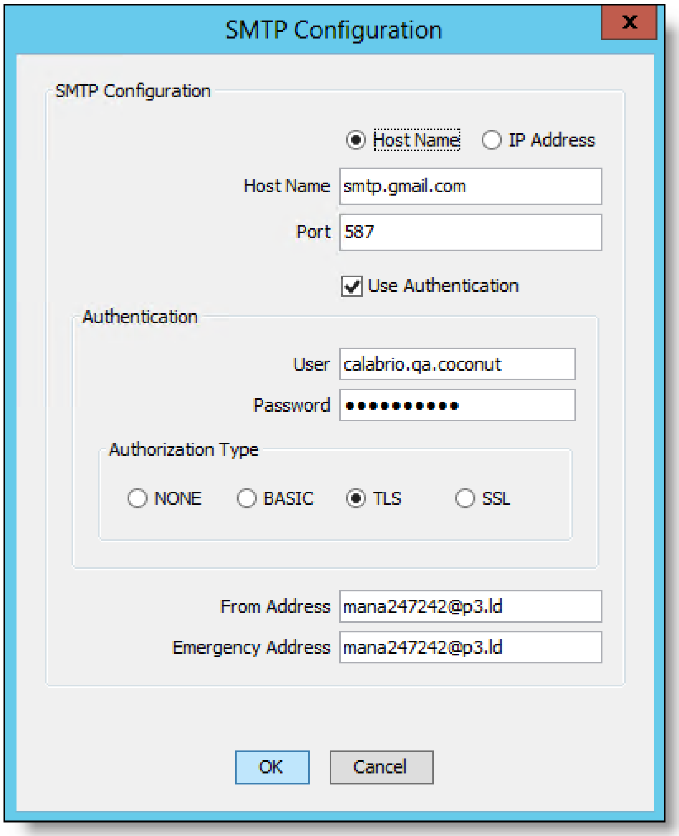
SMTP Configuration

SMTP Configuration allows you to configure the SMTP email connection.

Note: This feature is only enabled on the Web Base server.

Notifications can be sent to 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. If you are using email notification, you must configure SMTP. This can be done only from the Quality Management Web Base server.



SMTP Configuration

SMTP Configuration

● Host Name ○ IP Address

Host Name smtp.gmail.com

Port 587

☑ Use Authentication

Authentication

User calabrio.qa.coconut

Password ●●●●●●●●●●●

Authorization Type

○ NONE ○ BASIC ● TLS ○ SSL

From Address mana247242@p3.ld

Emergency Address mana247242@p3.ld

Field	Description
Host Name/IP Address	Choose Host Name or IP Address, and then enter the hostname or IP address of the SMTP server. **Best Practices:** Use a hostname in all instances where you are required to specify a hostname or IP address, if possible.
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 required to access the SMTP server.
Password	The password required to access the SMTP server.

Field	Description
Authorization Type	The type of authorization required. Your options are as follows: ■ NONE ■ BASIC ■ TLS ■ SSL
From Address	The email address from which all notifications will come.
Emergency Address	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. 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.

To configure SMTP settings for email:

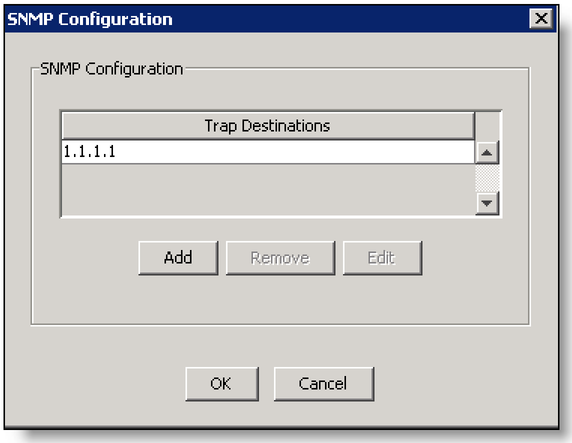
- Click SMTP Configuration, complete the fields, and then click OK.

SNMP Configuration

SNMP Configuration allows you to configure the Simple Network Management Protocol (SNMP) connection.

> **Note:** This feature is only enabled on the Web Base server.

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



Field	Description
Trap Destinations	The available trap destinations.
Add	Add a trap destination.
Remove	Remove a trap destination.
Edit	Edit a trap destination.

To configure SNMP settings for notification:

- 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 click Remove to delete IP address.

Restart the Windows SNMP service to enable your changes.

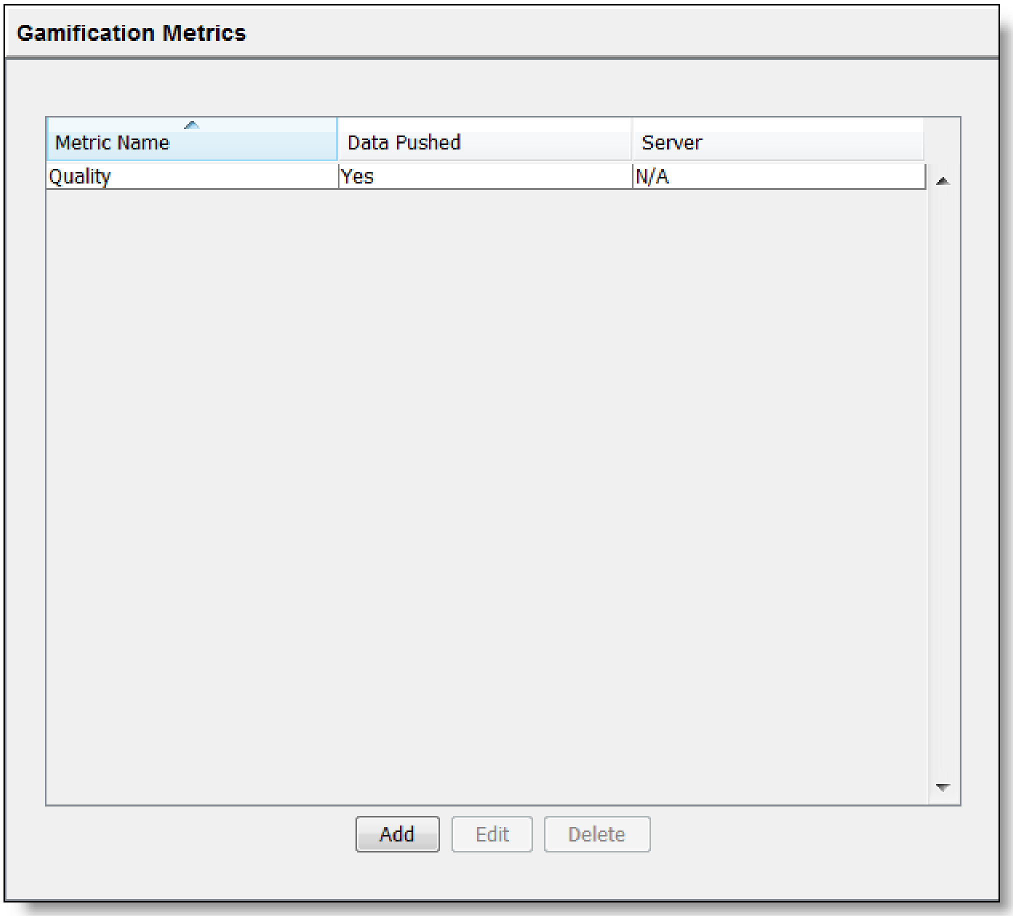
> **Note:** You must restart the SNMP service any time you make a change in trap destinations, including on the initial setup.

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*.

Gamification Metrics

Use the Gamification Metrics window to configure the connection settings to allow the retrieval or posting of gamification metrics. Additional configuration options are provided in Recording and Quality Management when you log in to Unified Workforce Optimization.



Gamification Metrics

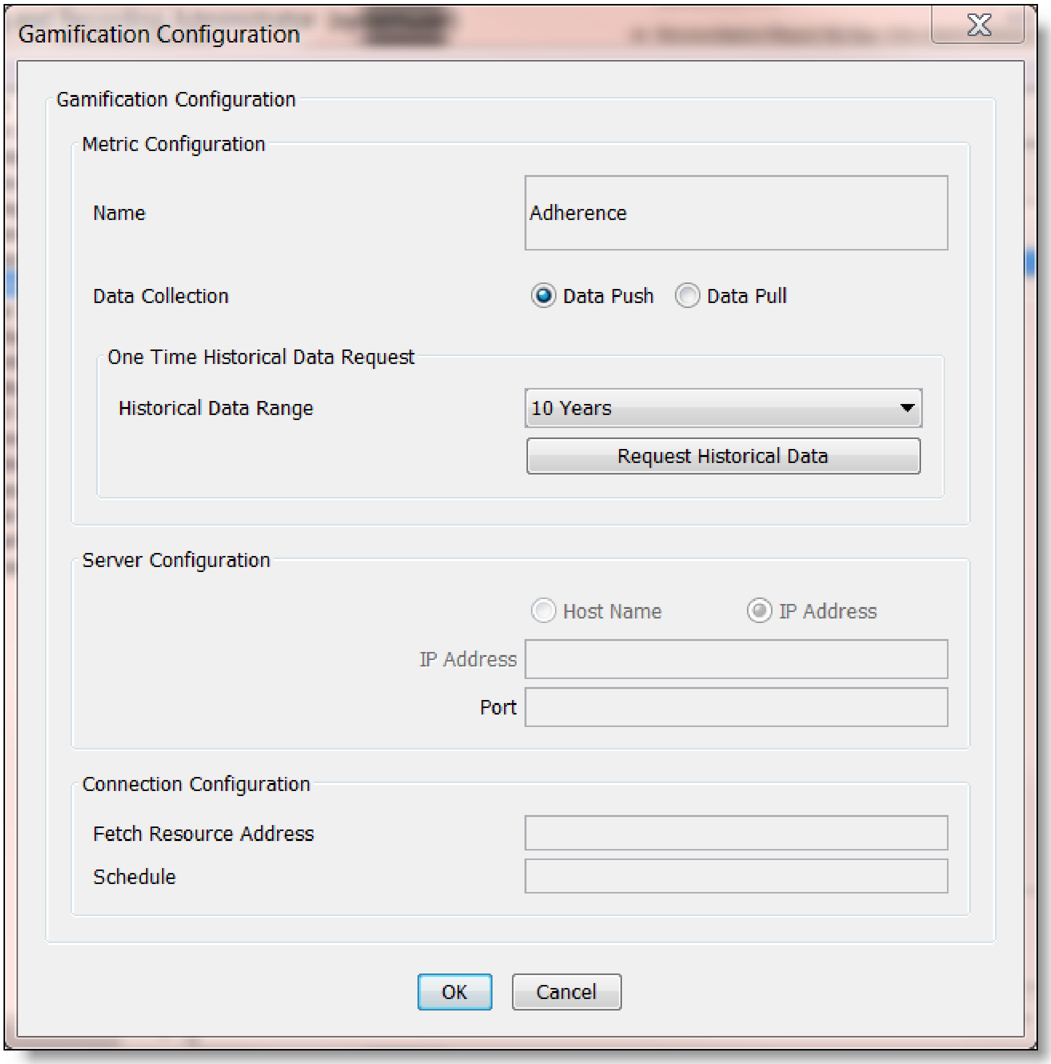
Metric Name	Data Pushed	Server
Quality	Yes	N/A

The default metric for this window is Quality; you can add one or more additional metrics, either Quality or Adherence.

Field or Button	Description
Metric Name	The name of the metric. The available metrics are as follows: ■ Adherence–the agents' adherence data. This metric is pulled from WFM and requires additional configuration. Once configured, Quality Management will retrieve the nightly, as well as historical performance data from WFM. ■ Quality–the agents' performance data from evaluations. This metric is pushed from Recording and Quality Management and required no additional configuration.
Data Pushed	Indicates how the data is collected. The options are as follows: ■ Yes–the data is pushed (or posted) ■ No–the data is retrieved (or pulled)
Server	The hostname or IP address of the server.
Add	Add a new metric.
Edit	Modify a selected metric.
Delete	Remove a selected metric.
Type	Select the metric type (Adherence). When you click Add, the Add Gamification Metric dialog box displays this field.

Gamification Configuration

Use the Gamification Configuration dialog box to configure the connections settings for a selected metric.



Gamification Configuration

Gamification Configuration

Metric Configuration

Name: Adherence

Data Collection: ● Data Push ○ Data Pull

One Time Historical Data Request

Historical Data Range: 10 Years

Server Configuration

○ Host Name ● IP Address

IP Address:

Port:

Connection Configuration

Fetch Resource Address:

Schedule:

Field or Button	Description
Name	The name of the metric. The available metrics are as follows: ■ Adherence—the agents' adherence data. This metric is pulled from WFM and requires additional configuration. Once configured, Quality Management will retrieve the nightly, as well as historical performance data from WFM. ■ Quality—the agents' performance data from evaluations. This metric is pushed from Recording and Quality Management and required no additional configuration.
Data Collection	Choose one of the following options: ■ Data Push—When you select this option, the data is pushed (or posted) to the specified server. ■ Data Pull—When you select this option, the data is retrieved or pulled from the specified server.
Historical Data Range	Select an historical date range from the drop-down list. This field is enabled when you select Data Push.
Request Historical Data	When clicked, Quality Management pushes historical data to the specified server. This button is enabled when you select Data Push.
Server Configuration Hostname or IP Address	The hostname or IP address of the server container for the gamification metric. This field is enabled when you clear the Data Push check box. For the adherence metric, specify the hostname or IP address of the WFM container.
Server Configuration Port	The port number for the server for the gamification metric. This field is enabled when you clear the Data Push check box.
Connection Configuration Fetch Resource Address	The location of the API where the performance data will be retrieved from. When you choose the Adherence metric, this field is prepopulated with the path to the performance data and cannot be changed.

Field or Button	Description
Connection Configuration Schedule	The schedule for retrieving the performance data. By default the value is * * * * *. You can adjust the retrieval schedule to suit your needs. This field accepts a free form text value of the cron formatted (http://www.nncron.ru/help/EN/working/cron-format.htm) schedule.

Managing Gamification Metrics

To update connection details for a metric:

- Click Update Connection Details, complete the fields in the Gamification Configuration dialog box, and then click OK.

Administrator Configuration

Note: When you upgrade to 11.5 from 10.5 or earlier, the only administrator that exists will be the default administrator. The default administrator is a system administrator. Users who were assigned the administrator role in10.5or earlier will require additional configuration. After upgrading to 11.5, you need to assign your administrator users based on the new hierarchical administrative roles.

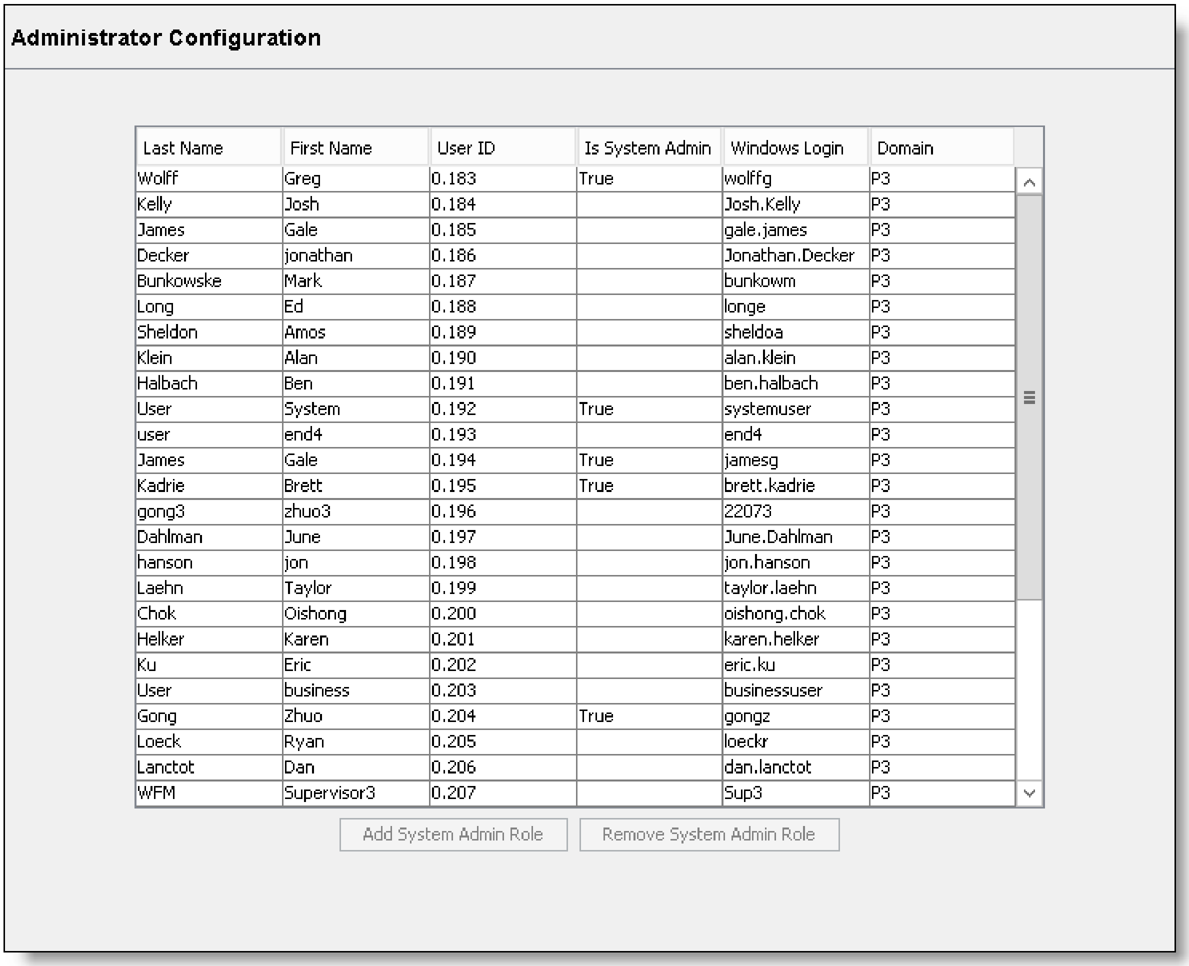
The Administrator Configuration window allows you to assign the system administrator role to users who belong to the Admin Group. See the *Domain Information* for a description of the Admin Group and "Administrator" in the *Administrator Guide* for a description of the administrator roles.

Important: Once you assign the system administrator role to a user in a non-Active Directory environment, the default administrator user becomes obsolete and you can no longer log in as a default administrator.

Note: You can only promote users to system administrator from postinstall.exe on the Web Base server.

If you *are* using Active Directory, the Administrator Configuration window will only display users in the security group that have a complete configuration (including a Last Name).

If you *are not* using Active Directory, the Administrator Configuration window will display users configured in the User Administration window.



Administrator Configuration

Last Name	First Name	User ID	Is System Admin	Windows Login	Domain
Wolff	Greg	0.183	True	wolffg	P3
Kelly	Josh	0.184		Josh.Kelly	P3
James	Gale	0.185		gale.james	P3
Decker	jonathan	0.186		Jonathan.Decker	P3
Bunkowske	Mark	0.187		bunkowm	P3
Long	Ed	0.188		longe	P3
Sheldon	Amos	0.189		sheldoa	P3
Klein	Alan	0.190		alan.klein	P3
Halbach	Ben	0.191		ben.halbach	P3
User	System	0.192	True	systemuser	P3
user	end4	0.193		end4	P3
James	Gale	0.194	True	jamesg	P3
Kadrie	Brett	0.195	True	brett.kadrie	P3
gong3	zhuo3	0.196		22073	P3
Dahlman	June	0.197		June.Dahlman	P3
hanson	jon	0.198		jon.hanson	P3
Laehn	Taylor	0.199		taylor.laehn	P3
Chok	Oishong	0.200		oishong.chok	P3
Helker	Karen	0.201		karen.helker	P3
Ku	Eric	0.202		eric.ku	P3
User	business	0.203		businessuser	P3
Gong	Zhuo	0.204	True	gongz	P3
Loeck	Ryan	0.205		loeckr	P3
Lanctot	Dan	0.206		dan.lanctot	P3
WFM	Supervisor3	0.207		Sup3	P3

Field or Button	Description
Last Name	The user's last name.
First Name	The user's first name.
User ID	
Is System Admin	When True appears in the field, the user is assigned to the system administrator role. A blank field indicates the user is not a system administrator. To assign the business or telephony administrator role to a user, see "User Administration" in the *Administrator Guide*.
Windows Username	The user’s Windows user name.

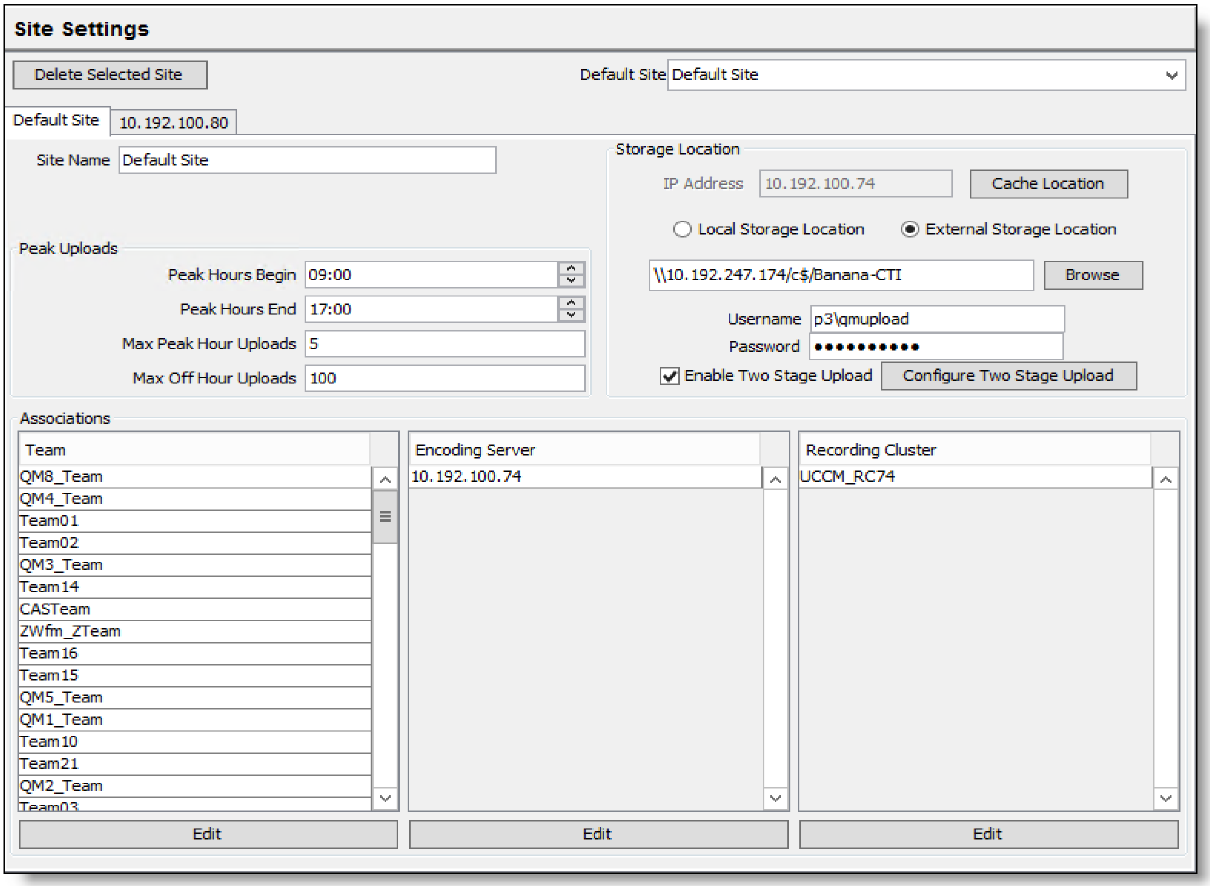
Field or Button	Description
Domain	The user's domain name.
Add System Admin Role	To assign the system administrator role, select one or more users who are not system administrators and click the Add System Admin Role button.
Remove System Admin Role	To remove the system administrator role, select one or more users who are system administrators and click the Remove System Admin Role button.

Managing Administrators

- To assign the system administrator role, select one or more users who are not system administrators and click the Add System Admin Role button.
- To remove the system administrator role, select one or more users who are system administrators and click the Remove System Admin Role button.

Site Settings

Use the Site Settings window to configure one or more sites and associate teams and Recording Clusters with each site.



Site Settings

Default Site: Default Site

Tabs: Default Site | 10.192.100.80

Site Name: Default Site

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: 10.192.100.74
- ○ Local Storage Location ● External Storage Location
- \\10.192.247.174/c$/Banana-CTI
- Username: p3\qmupload
- Password: ●●●●●●●●●●
- ☑ Enable Two Stage Upload

Associations

Team	Encoding Server	Recording Cluster
QM8_Team	10.192.100.74	UCCM_RC74
QM4_Team		
Team01		
Team02		
QM3_Team		
Team14		
CASTeam		
ZWfm_ZTeam		
Team16		
Team15		
QM5_Team		
QM1_Team		
Team10		
Team21		
QM2_Team		
Team03		

When you install the Site Upload Server on a server, this is the first screen to appear in 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 Encoding Servers from a site
- Add or remove Recording Clusters from a 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
- Configure storage locations
- Enable and configure two stage upload

Field	Description
Delete Selected Site	Remove an existing site.
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.
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.

Field	Description
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. If you change the storage location, you must run the Set Recording Home Directory tool to restart the services. **Note:** If you are using remote storage, the Media API 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.
Cache Location	(Cloud-based storage only) The location where unencrypted voice and screen recordings are stored. These files are used for playback. The specified directory must be accessible by the local system users and each of the Encoding servers. External location credentials must be shared with the permanent storage location. A cache location is required if you are using cloud-based storage. Unencrypted files must be stored separate from the permanent storage location for performance reasons. Note that the Jetty service must be restarted when you change the cache location for the changes to go into effect.
Local Site Cache Location	Choose this option to store the unencrypted voice and screen recording in a local site cache location. **Best Practices:** If there is only one configured Media Encoder and it is local, choose the Local Site Cache Location for best performance.

Field	Description
External Site Cache Location	Choose this option to store the unencrypted voice and screen recording in an external site cache location. **Best Practices** If there are one or more Media Encoders and they are not local, choose the External Site Cache Location. You can specify any network location accessible to the Jetty services and all Media Encoder services configured for this site.
Site Cache Location Username	Enter the username required to access the site cache location. This user must meet these requirements: ■ The site cache location 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 site cache location. This means the site cache location 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 site cache drive location entered AND the location where Quality Management is installed on the local server. **Note:** The Jetty and Media Encoder services must be running as this user.
Site Cache Location Password	Enter the password required to access the site cache location.
Local Storage Location	Choose this option to store the voice and screen recordings on the Quality Management server.

Field	Description
External Storage Location	Choose this option to store the voice and screen recordings on an external server. **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).
Storage Location Path	The path where voice and screen recordings are stored. Click Browse and navigate to the storage folder. **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).
Browse	Locate a folder.

Field	Description
Storage Location Username	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>. 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. This user must meet these requirements: ■ 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 Recording 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.
Storage Location Password	If you selected an external storage location, enter the password required to access that location.

Field	Description
Enable Two Stage Upload	When selected, two stage upload is enabled. Two stage upload immediately uploads screen and audio recordings to a temporary storage location. You can then configure a workflow to upload files from the temporary storage location to the permanent storage location at the End of Day. Two stage upload functions in one of two manners: 1. If you are using Desktop Recording (or Gateway Recording), the Desktop Recording service will round robin through all Recording Servers associated with the site. This will happen regardless of the location of the Recording Servers. If you are using Desktop Recording and need to limit your uploads to a local Recording Server, you will need to configure a site for that location. 2. If you are using Server Recording, the Desktop Recording service will round robin through Recording Servers that are in the same cluster as the agents. All recordings will go to your local Recording Cluster. If no configuration information is available for your local Recording Cluster, no recordings will upload from those agents. Enable two stage upload when: ■ Your contact center has multiple sites that are separated by a WAN and you want to use the Immediate Upload feature but you have limited bandwidth. ■ You are using Desktop Recording and your contact center requires the agents to shut down their desktop at the end of a shift. Shutting down the desktop interrupts the scheduled upload based on the agent's workflow. Two stage upload ensures the recordings are immediately uploaded to the temporary storage location after a call. On startup, the Desktop Recording service retrieves all site information, including all two stage upload locations. When a call ends, recordings are moved to a temporary

Field	Description
	storage location and then uploaded to the permanent storage location. The files are moved in the following order: voice, screen, ini. If there are no two stage upload locations, two stage uploads are turned off. Recordings are uploaded using the round-robin method to the available storage locations. **Note:** When two stage upload is enabled, it is possible that voice and screen recordings for a call might be stored in different storage locations. When cleared, recordings are uploaded directly to the central storage location. When the upload occurs is determined by the workflow assigned to the agent. This check box is only enabled when at least one Recording Cluster is assigned to the site.
Configure Two Stage Upload	Click this button if you want to configure a temporary storage location. The Two Stage Upload Configuration dialog box will display the Recording Servers associated with the Recording Clusters assigned to the site. Click the Modify button associated with the selected server to configure the UNC path, username, or password to that server. This button is enabled when you select Enable Two Stage Upload and at least one Recording Cluster is assigned to a site.
Two Stage Upload Configuration Server	The IP address or hostname of the of the Recording server that hosts the temporary storage location. This field appears in the Two Stage Upload Configuration dialog box.

Field	Description
Two Stage Upload Configuration UNC	The storage location path to the TwoStageLocation folder on the Recording server where voice and screen recordings are temporarily stored. The path must be in UNC format. The default path is as follows: \\<server>\TwoStageLocation where <server> is the IP address or host name of the Recording server that host the temporary storage location. The TwoStageLocation folder is automatically created the first time the Recording server is started. The default path is as follows on the Recording server: <temporary recording storage location>\TwoStageLocation where <temporary recording storage location> is the path to the temporary recording directory. See *Set Temporary Recording Directory* for more information. **Important:** The TwoStageLocation folder properties must be shared using Advanced Sharing and a username and password must be configured to access this folder. The user must be allowed the following permissions: Full Control, Change, and Read. Quality Management uses this path and the specified user name and passwords to access the TwoStageLocation folder. This field appears in the Two Stage Upload Configuration dialog box.
Two Stage Upload Configuration Username	Enter the username required to access the TwoStageLocation folder on the Recording server. This field appears in the Two Stage Upload Configuration dialog box.
Two Stage Upload Configuration Password	Enter the password required to access the TwoStageLocation folder on the Recording server . This field appears in the Two Stage Upload Configuration dialog box.

Field	Description
Modify	Click this button to modify the fields in the selected row. This button appears in the Two Stage Upload Configuration dialog box.
Team	A list of assigned teams.
Encoding Server	A list of assigned Encoding Servers.
Recording Cluster	A list of assigned Recording Clusters. **Note:** Assigning a Recording Cluster to a site takes precedence over a team. So a if a user is assigned to Team 1 on Site 1, but is associated with Recording Cluster A on Site 2, the recordings for that user will be uploaded to Site 2.
Edit	Modify the assigned teams, Encoding Servers, or Recording Clusters.

Site Considerations

If you plan to use multiple recording storage locations, you can associate each recording storage location to a site.

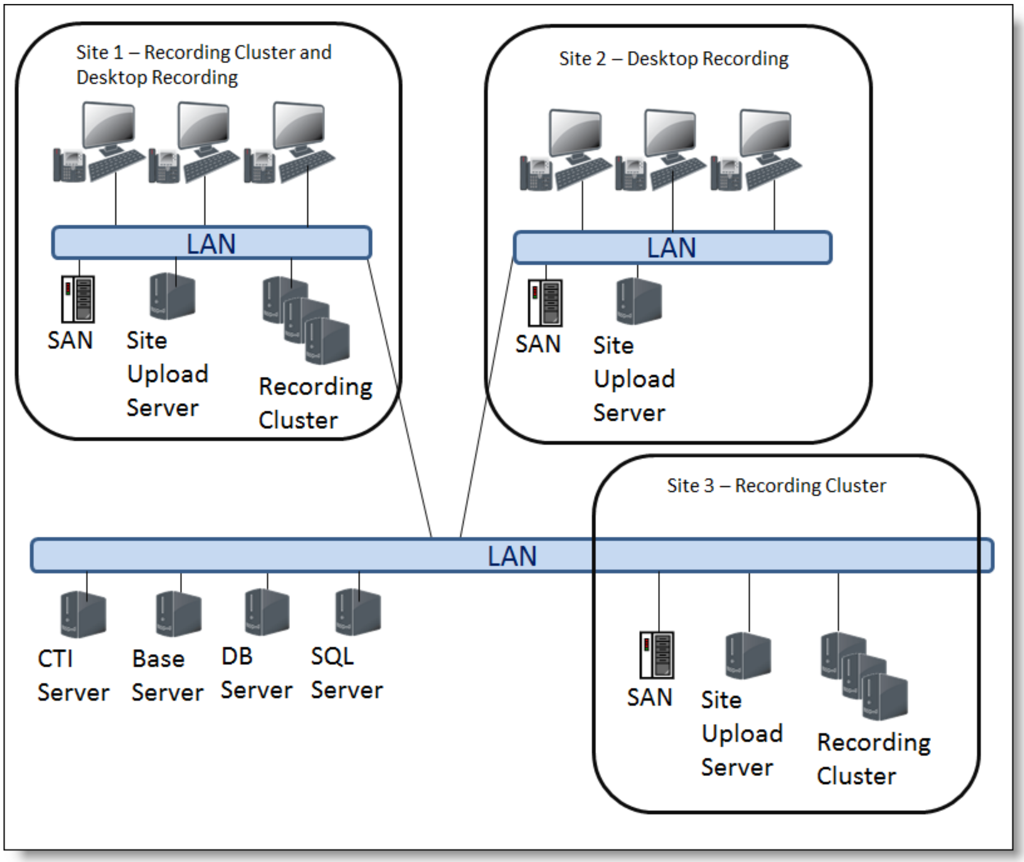
When configuring sites, consider the following:

- 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 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.

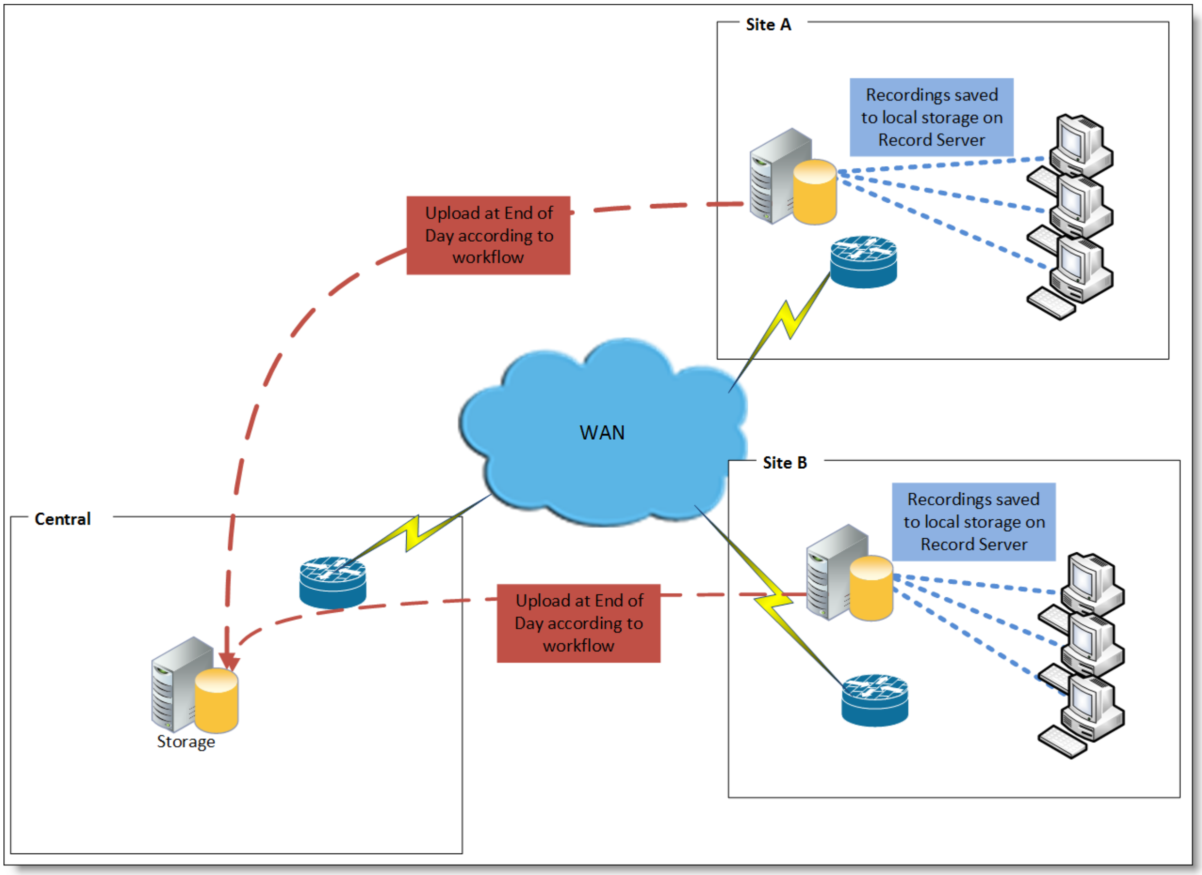
The following figure shows three sites—two external sites that communicate with the rest of the system over a WAN and one site that communicate over a LAN. Each site has a Site Upload server with an Upload Controller and a Recording Cluster. Each site has one or more teams assigned to it and the users in those teams will upload to the proper site.

Multiple site configuration example



Site recording storage location example: The Web 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.

The following figure shows two sites using two stage upload feature.


Site A
Recordings saved to local storage on Record Server
Upload at End of Day according to workflow
WAN
Central
Site B
Recordings saved to local storage on Record Server
Upload at End of Day according to workflow
Storage

Two stage upload example: Immediately after a call, Site A and Site B upload the recordings to their Recording server that hosts the temporary storage location. At the End of Day, the recordings are then uploaded to the permanent storage location.

Managing Site Settings

- To view the existing site configuration, click Site Settings.

  The Site Settings window appears.

- To view a different site, click the tab associated with the site.

  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:

  1. Click the tab for the site you want to remove.
  2. Click Delete Selected Site.
  3. Click Yes in the Confirm Delete dialog box.
  4. Choose where you want to move recordings from the deleted site, and then click OK.
  5. Manually remove the recording files stored at the deleted site, and then click OK.
  6. Open the Services window on the server and stop the following services:
     - Quality Management DB Proxy Service
     - Quality Management DB Cleaner Service
  7. Click OK in the Proceed? dialog box to continue.
  8. Click OK to dismiss the Save Successful dialog box.

  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 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:

  a. Complete the fields under Storage Location and then click Save.

  b. Select Tools > Set Recording Home Directory to restart the services.

- To enable two stage upload:

  a. Select Enable Two Stage Upload.

  b. Click Configure Two Stage Upload.

  c. Click Modify and complete the fields.

  d. Click OK.

- To modify the list of assigned teams, Encoding Servers, or Recording Clusters to a site, select the site’s tab, click Edit under Team, Encoding Server, or Recording Cluster, and choose one of the following options: select one or more teams, Encoding Servers, or Recording Clusters from the Teams, Encoding Servers, 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.

  - Add teams, Encoding Servers, or Recording Clusters. Click Edit under the option that you want to modify, select one or more items from the available list and click the > button to move the selected items to the assigned list, or click the >> button to move all items to the assigned list, and then click OK.

  - Remove teams, Encoding Servers, or Recording Clusters. Click Edit under the option that you want to modify, select one or more items from the assigned list and click the < button to move the selected items to the available list, or click the << button to move all items to the available list, and then click OK.

Configuration Settings Used By Services

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

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.
Media webapp (Jetty service)	Restart the Jetty service.

Service	Configuration settings applied when...
Network Recording service	If two stage upload is enabled and you move a Recording Cluster from one site to a different site, you must restart the Network Recording service for that Recording Cluster for the changes to take effect.

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.

This step must be done after you install the Quality Management Web Base Services and before you start recording contacts.

To enable external storage and services:

1. Create a username and password for the external storage user on the external storage server.
2. Configure the Jetty service for external storage.

To configure services for external storage:

1. Select Start > Administrative Tools > Services.

   The Services window appears.

2. Right-click Monitoring and Recording Jetty service and choose Properties.

   The Monitoring and Recording Jetty Service Properties window appears.

3. Click the Log On tab, choose This Account by providing the username and password for the external storage server, complete the fields, and then click Apply.

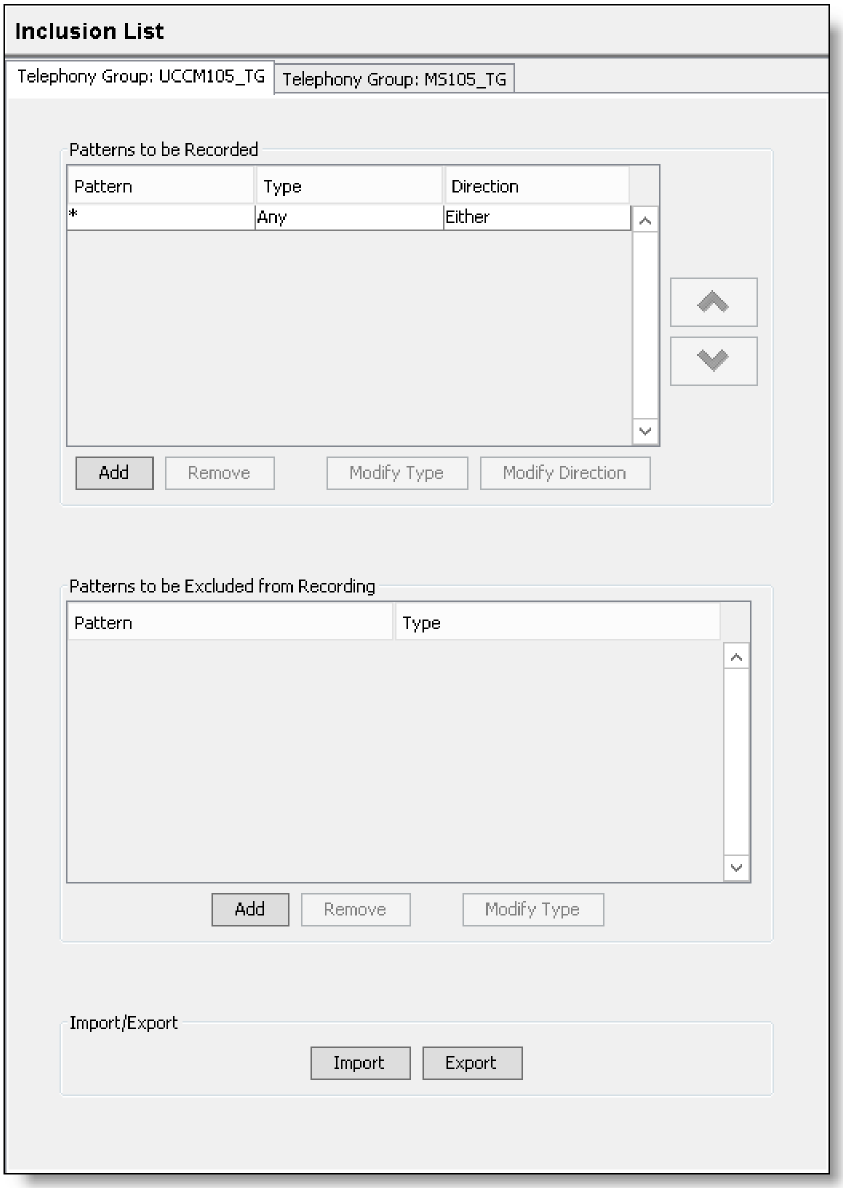
   If the provided information is correct, the following message will appear:

   ```
   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.

Inclusion List

Quality Management uses the Inclusion List window 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.



Patterns to be Recorded

Pattern	Type	Direction
*	Any	Either

Patterns to be Excluded from Recording

Pattern	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.

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

  See *Gateway Recording Considerations* and *Cisco MediaSense Recording Considerations* for more information.
- The type of call. Your options are:
  - Any—filters all called, calling, and extensions calls that match the extension pattern
  - Called—fillers 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
  - Excluded—excludes all inbound or outbound calls that match the extension pattern.

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.

You can also import or export an inclusion/exclusion list for a single telephony group. Changes to the inclusion/exclusion list take effect the next time the CTI service polls for configuration (five minutes at most). Importing or exporting a large inclusion/exclusion list is quick (Less than five seconds). However, it might take up 30 seconds to save a large inclusion/exclusion list to the database.

Any changes you make to the Inclusion List take window take effect at the next recording client login.

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.
Import	Allows you to select the location and name of an inclusion/exclusion file to import. The file must be in CSV format (see *Record Server Configuration* for more information). Importing an inclusion/exclusion list overwrites the existing file. An import does not merge changes. **Note:** If the CSV file has errors in it, the import will fail and the existing data will remain unchanged. An error message will indicate why the import failed and identify the record that failed if applicable. After importing a CSV file, you must click Save to save your changes.
Export	Allows you to select the location and specify a name for the exported inclusion/exclusion list. The file must be in CSV format. Once exported, you can open the file in Microsoft Excel.

CSV Format

The CSV file containing the inclusion/exclusion list must use the following format:

Pattern	Type	Bounds
A number pattern with optional * and ? wildcards	One of the following types: ■ Extension ■ Calling ■ Called ■ Any	One of the following directions: ■ Inbound ■ Outbound ■ Either ■ Excluded

When creating an inclusion/exclusion list, remember the following points:

- Exclusions are matched before inclusions, but exclusions can appear anywhere in the CSV.
- Within each group (inclusions and exclusions), patterns are matched starting from the top and working down the list.
- Additional columns after Pattern, Type, and Bounds are allowed in an imported CSV. However, the additional columns will be ignored.

Gateway Recording Considerations

The considerations in this topic apply to the following Gateway Recording method:

- Cisco CUBE Recording via SIP Recording

When the call direction cannot be determined, the Inclusion List will only match a Direction with a value of Either. All calls, both inbound and outbound, appears as inbound. Cisco recommends setting the value of the Direction to Either when creating an exclusion for a Gateway Recording method.

Cisco MediaSense Recording Considerations

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.

When configuring the Inclusion List for Cisco MediaSense Recording, consider the following:

- The entire call is recorded and saved on the Cisco MediaSense Recording cluster.
- Quality Management only downloads Cisco MediaSense recordings that appears in the Patterns to be Recorded list.
- Quality Management does not download Cisco MediaSense recordings that appear in the Patterns to be Excluded from Recording list.

- When the call direction cannot be determined, the Inclusion List will only match a Direction with a value of Either. Cisco recommends setting the value of the Direction to Either when creating an exclusion for Cisco MediaSense Recording.

Managing Extension Patterns

To manage extension patterns:

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. **Example:** 6124, 61555, 613
61??	Any number that start with 61 and are 4 digits long. **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.
   - Import an inclusion/exclusion list. Click Import, select the location, the file name of the inclusion/exclusion list, click OK, and then click Save.

- Export an inclusion/exclusion list. Click Export, select the location, type the file name of the inclusion/exclusion list, and then click OK.

3. Click Save.

Excluding Extension Patterns

If you have a limited number of extension patterns you want to exclude from being recorded, you can configure the Inclusion List to ignore only those extension patterns and record all others.

> **Example:** If you want to record all extension patterns except for extensions 3411, 3412, and 3413, configure your inclusion list so that there is an asterisk in the Patterns To Be Recorded list, and extensions 3411, 3412, and 3413 listed in the Patterns To Be Excluded From Recording list.

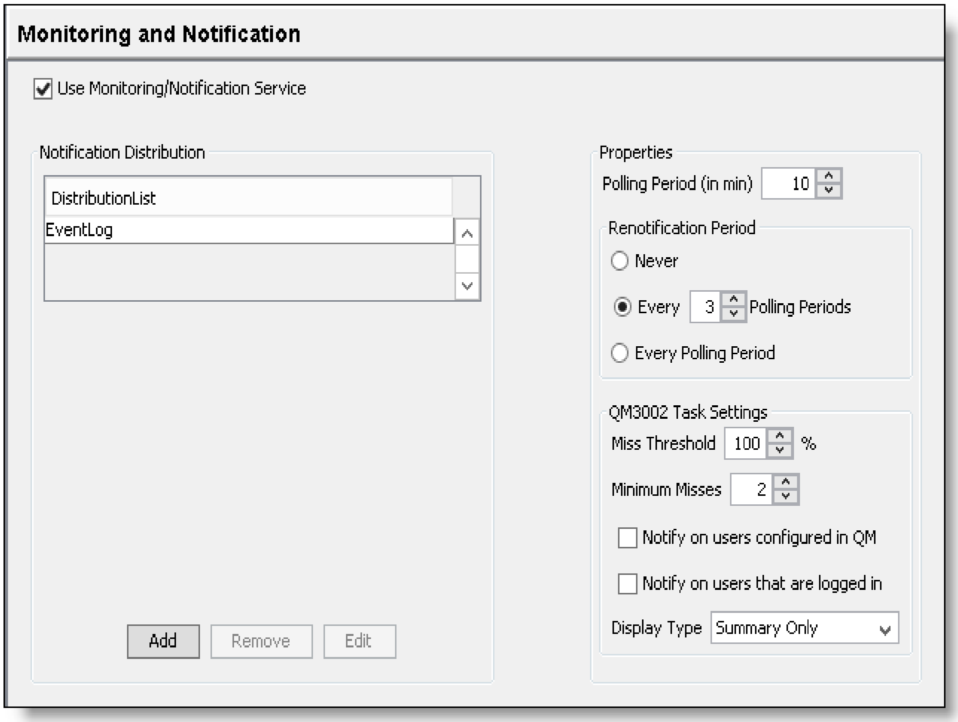
Extension patterns listed in the Patterns To Be Excluded From Recording list always take precedence over extension patterns listed in the Patterns To Be Recorded section. You cannot use the same extension pattern (specifically or through the use of wildcards) in both lists.

> **Example:** 12* cannot appear in both lists.

Monitoring and Notification

Use the Monitoring and Notification window to enable the Monitoring and Notification (MANA) service and add a distribution list for notifications.

The following image displays the Monitoring and Notification window for Unified CCX.



Monitoring and Notification

☑ Use Monitoring/Notification Service

Notification Distribution

DistributionList
EventLog

Properties

Polling Period (in min) 10

Renotification Period

○ Never

● Every 3 Polling Periods

○ Every Polling Period

QM3002 Task Settings

Miss Threshold 100 %

Minimum Misses 2

□ Notify on users configured in QM

□ Notify on users that are logged in

Display Type Summary Only

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 versions 8.x+ and 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.

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 postinstall.exe or Quality Management Administrator on the Web Base server. The Monitoring and Notification window in Quality Management Administrator on a desktop is read-only.

Connection information is saved locally to the Web 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.

Field or Button	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.
Add	Add a distribution list.
Remove	Remove a distribution list.
Edit	Edit the selected distribution list.
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.

Field or Button	Description
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.
QM 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.
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 a desktop where the Desktop Recording service is installed. This only applies to the Desktop Recording service.
Display Type	Choose one of the following options. ■ Summary Only—displays 1 row per agent with missed CDR that meet the above criteria. See Summary Only for an example. ■ Details (Tab Delimited)—displays each missed CDR in tab delimited format. See *Detail (Tab Delimited)* for an example. ■ Details (Plain Text)—displays each missed CDR in text format. See *Detail (Plain Text)* for an example.

Configuration Settings Used By Services

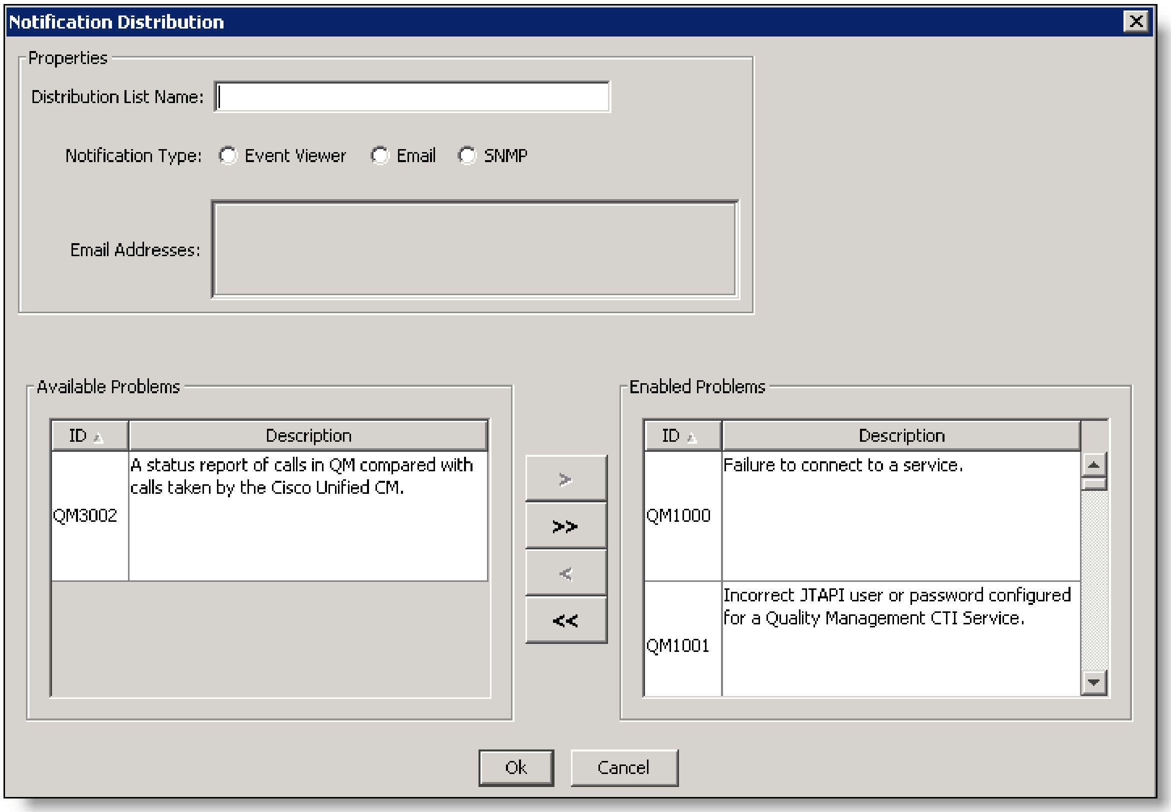
If you change the settings on the Monitoring and Notification window, the following table shows when your changes take effect.

Service	Configuration settings applied when...
MANA service	The next polling period applies the configuration settings.

Notification Distribution

The Notification Distribution dialog box allows you to create a distribution list, specify the notification type for the distribution list, and assign the type of MANA alerts that are sent to the distributions list.

The following image displays the Notification window for Unified CCX.



ID	Description
QM3002	A status report of calls in QM compared with calls taken by the Cisco Unified CM.

ID	Description
QM1000	Failure to connect to a service.
QM1001	Incorrect JTAPI user or password configured for a Quality Management CTI Service.

The MANA alerts 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.

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: ■ 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. A comma is required to separate two or more email addresses. **Example:** jane.doe@acme.com, john.smith@acme.com, robert.dee@acme.com **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. QM3002 appears in this list by default.
Enabled Problems	The list of problems that will trigger notification. By default, all problems are enabled, except for QM3002. You must configure QM3002 under QM Task Settings in the Monitoring and Notification window before you can enable this Call Detail Record (CDR) task. **Note:** QM3002 is not supported with Cisco MediaSense Recording.

Managing Notification Distribution Lists

To manage notification email addresses:

- To add a distribution list, perform the following steps.
  - Click Add in the Notification Distribution section.
  - Type the name of the distribution list in the Distribution List Name field.
  - Type the email addresses that are included in the distribution list in the Email Addresses field.
  - Move the type of problems you want sent to this distribution list to the Enabled Problems list.
  - Click OK.

  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.

  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.

Installation Complete

Start Services

Click Yes to start services.

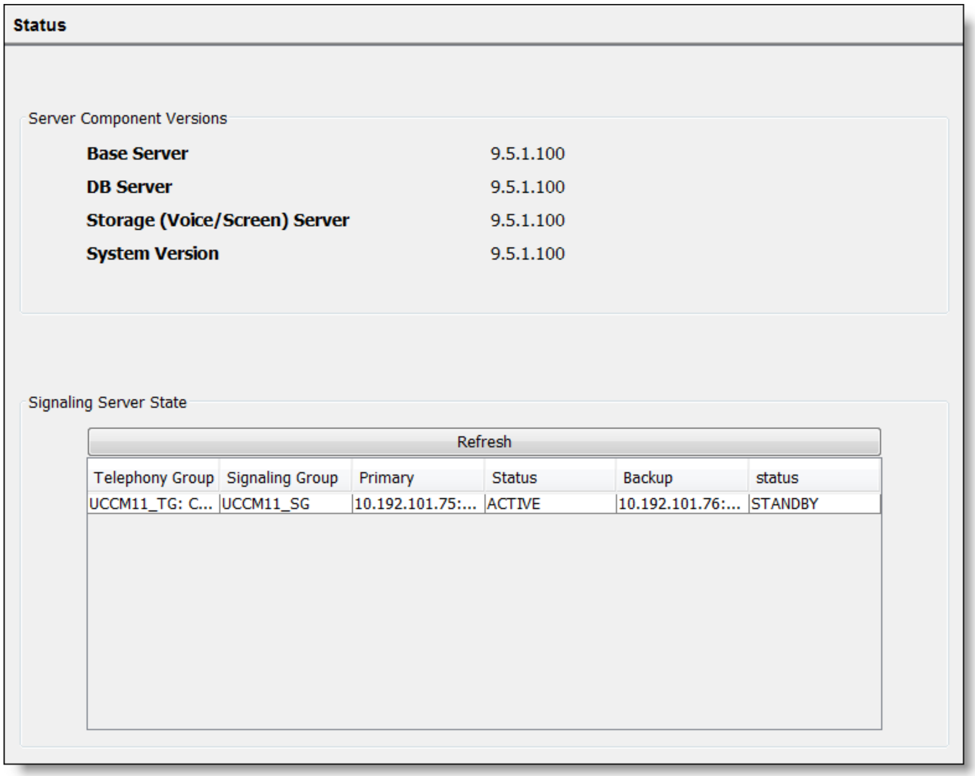
The program starts the services for Quality Management. When finished, the Services Started Successfully confirmation box appears.

Services Started Successfully

Click OK to dismiss the confirmation box.

Status

The Status window reports the version of the installed Quality Management components and displays the status of the signaling servers by telephony group. Click refresh to see the latest signaling server information.



Status

Server Component Versions

Base Server	9.5.1.100
DB Server	9.5.1.100
Storage (Voice/Screen) Server	9.5.1.100
System Version	9.5.1.100

Signaling Server State

Telephony Group	Signaling Group	Primary	Status	Backup	status
UCCM11_TG: C...	UCCM11_SG	10.192.101.75:...	ACTIVE	10.192.101.76:...	STANDBY

Configuration Settings Used By Services

If you change the product version, the following table shows when your changes take effect.

Service	Configuration settings applied when...
Upload Controller service	Periodically check for a version mismatch.

Manually Installing the Cisco JTAPI Client

Follow the instructions in this task only if the postinstall.exe did not automatically install the Cisco JTAPI Client in the Cisco environment.

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

To manually install the Cisco JTAPI Client:

1. Stop the Recording CTI service or CUBE SIP 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 or CUBE SIP 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

   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 or CUBE SIP CTI service.
6. Start postinstall.exe in C:\Program Files\Cisco\WFO_QM\bin.
7. Choose Tools > Test CTI Service.

   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.

Rules for Upgrading or Modifying the ACD Database in Update Mode

Observe the following rules when you change access to the Unified CCX Administration database in update mode:

- Do not change the location of the Unified CCX Administration 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 Administration database.

Stopping the Sync Service Before Upgrading the ACD Database

Perform this task before you upgrade the Unified CCX Administration database.

To stop the Sync service:

1. Select Start> Administrative Tools > Services. 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.

   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 Administration 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.

   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 Administration database. Failing to do so could potentially deactivate users if there is a problem with the Unified CCX Administration upgrade or rebuild.
8. Verify the teams and agents in the upgraded Unified CCX Administration appear correctly.

Changing the Web Base Server

To change the IP address or host name for the Web Base server:

1. From the postinstall.exe, choose File > Choose Base Server.

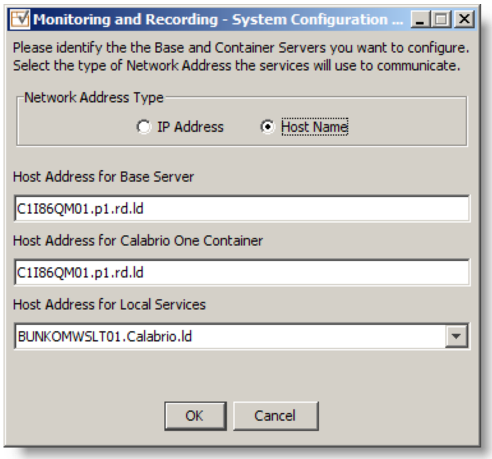
   The System Configuration Setup dialog box appears window appears.

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.

    The base server is the computer where you installed the Web Base Services, Database Services, Voice/Screen Services, and signaling service.
4. Enter the IP address or hostname of the Unified Workforce Optimization Container.

    The Unified Workforce Optimization Container is located on the base server.

    If you also purchased WFM, this product will share this container once it is configured to point to this container. The following figure displays the System Configuration Setup dialog box.



Monitoring and Recording - System Configuration ...

Please identify the the Base and Container Servers you want to configure.
Select the type of Network Address the services will use to communicate.

Network Address Type

○ IP Address ● Host Name

Host Address for Base Server

C1I86QM01.p1.rd.ld

Host Address for Calabrio One Container

C1I86QM01.p1.rd.ld

Host Address for Local Services

BUNKOMWSLT01.Calabrio.ld

5. Choose one of the following options:
    - If you are running postinstall.exe 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 postinstall.exe on a different server, choose the IP address or hostname for the server from the Local Services drop-down list, and then click OK.

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.

To change the configuration data in update mode:

1. Start postinstall.exe.

   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.

   System Configuration Setup closes.

4. Stop and restart the modified service and all desktops for the change to go into effect.

Managing Certificates

Quality Management supports HTTPS using a self-signed certificate. The self-signed certificate is sufficient to encrypt the communication path between the Quality Management server and the client browsers, however it has the following limitations:

- Agents see a certificate error or security alert the first time they access Unified Workforce Optimization.
- User security is not complete. Users are vulnerable to a man-in-the-middle attack (an active form of eavesdropping where private communication is controlled by a hacker).
- Errors appear when using HTTPS if you use WFO Finesse gadgets.

You can update the certificate so that users are not required to accept self-signed certificates. This prevents the possibility of man-in-the-middle attacks.

Important: For a deployment that includes multiple Unified Workforce Optimization products, if every user connects to Unified Workforce Optimization on the Analytics Web Base server, then you only need to update the certificate on that Web Base server. Follow the instructions in this section only if Analytics is not connected to the Analytics Web Base server and you want to use an HTTPS URL and a self-signed certificate to access Unified Workforce Optimization.

Requirements

Follow these steps to update the Quality Management signed certificate. You will need the following to perform this procedure :

- keytool.exe, located in the Cisco\WFO_QM\Java bin directory

  Example: `C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe`

- A Certificate Authority (CA) from a commercial service, like Symantec VeriSign or GoDaddy, or a local CA like Microsoft Active Directory Certificate Services (AD CS).

Updating the Quality Management Signed Certificate

To update the Quality Management Signed Certificate:

Important: You will need to delete the existing certificate in the following situations:

If you are installing or upgrading from Quality Management 10.5 or earlier
The certificates for version 10.5 identify the country code as USA. You need to delete this certificate and regenerate it with the correct country code of US.

If you are installing or upgrading from Quality Management 10.5 or earlier and you want a stronger signature algorithm
Starting with version 11.5, self-signed certificates are created using SHA256withRSA. Previously, the default for self-signed certificates was MD5withRSA, and sha1WithRSA was suggested for signed certificates.

1. Log in to the Quality Management Web Base server with administrator rights.
2. From the command line (cmd.exe), enter the following command to delete the existing certificate:

   ```
   "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
   "C:\Program Files\Common Files\QM\config\.keystore" -storepass
   C@labr1o -delete -alias jetty
   ```

3. Enter the following command to create the correct certificate. In the example below, the command uses SHA2 encryption (there are multiple commands for creating the correct certificate; your command may vary).

   Note: Cisco supports signature algorithms defined by Java 8. Refer to the Oracle Java 8 documentation for a complete list of algorithms: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#Signature

   Note: Replace <IP Address> in the following command with the IP address of the Web Base server before you enter the command.

   Example:
   ```
   C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -
   keystore "C:\Program Files\Common Files\QM\config\.keystore" -
   storepass C@labr1o -selfcert -genkey -keyalg RSA -alias jetty -
   keysize 2048 -dname "C=US, S=MN, L=Minneapolis, O=Cisco,
   ```

```
OU=Quality Management, CN=<IP Address>" -sigalg sha256WithRSA -
validity 1000000 -v
```

4. Press Enter when the Enter key password for <jetty> prompt appears.
5. Restart the Jetty service on the Web Base server from Start > Control Panel > System and Security > Administrative Tools > Services.
6. Verify the certificate works by entering the following URL in your browser:

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

   where < Web Base server> is the host name or IP address of the server that hosts the Unified Workforce Optimization Container.

   A security warning will appear but you should still be able to log in to Unified Workforce Optimization with a valid username and password.

Creating a Certificate Signing Request (CSR) for the Web Base Server

To create a Certificate Signing Request (CSR) for the Web Base server:

1. From the command line on the Web Base server, enter one of the following commands:
   - If the users will access Unified Workforce Optimization using an IP address, use:

     ```
     "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -
     keystore "C:\Program Files\Common
     Files\QM\config\.keystore" -storepass C@labr1o -certreq -
     alias jetty -file jetty.csr
     ```

     This command generate a CSR for Quality Management.
   - If the users will access Unified Workforce Optimization using one or more domain names, use:

     ```
     "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -
     keystore "C:\Program Files\Common
     Files\QM\config\.keystore" -storepass C@labr1o -certreq -
     ```

```
alias jetty -file jetty.csr -ext
san=dns:<myDomain>,dns:<yourDomain>
```

For information on using IP addresses in this instance, see Using an IP address for a SAN in Internet Explorer.

Note: If you want to include multiple domains, use a comma to separate each domain.

This command uses the keytool -ext option to specify multiple domain names.

Example:
```
"C:\Program Files\Cisco\WFO_
QM\Java\bin\keytool.exe" -keystore "C:\Program
Files\Common Files\QM\config\.keystore" -storepass
C@labr1o -certreq -alias jetty -file jetty.csr -ext
san=dns:qmcert.pdi.ld,dns:qmcert2.pdi.ld
```

The jetty.csr resides in the following location:

```
C:\Users\<username>
```

where <username> is the login name for the user with administrator rights.

Certificates and Commercial Services

You can generate signed Quality Management certificates using commercial services such as VeriSign, Thawte, or GoDaddy.

The following topics describe how handle certificates from commercial services:

- *Generating Certificates Using Commercial Services*
- *Expired Certificate from a Commercial Service*

Generating Certificates Using Commercial Services

Step 1: Submit the CSR to your Certificate Authority.

The procedure for obtaining a signed Quality Management certificate varies by vendor. Consult your chosen vendor's website for instructions for requesting a signed certificate.

Note: Your CA will return to you a signed Quality Management certificate, and possibly one or more intermediate certificates.

See *Expired Certificate from a Commercial Service* for additional information.

Step 2: Import the root certificate from the Certificate Authority into the Quality Management keystore.

Import the CA root and any intermediate certificates into the keystore. These certificates can be acquired from the CA used to generate the signed Quality Management certificate.

Note that you might not need these certificates if they are already part of the Java cacerts store like VeriSign or Thawte. Lesser known CAs like GoDaddy, or an internal AD CS, will need to be installed on the Web Base server and also on the client web browser.

1. Log in to the Quality Management Web Base server with administrator rights.

2. From the command line on the Web Base server, enter the following command:

   ```
   "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
   "C:\Program Files\Cisco\WFO_QM\Java\lib\security\cacerts" -
   storepass changeit -list -v
   ```

   This command lists the existing CA certificates that comes bundled with QM Java.

   Note: If your CA appears in this list, you do not need to install it.

3. If your root certificate is not already installed, enter the following command:

   ```
   "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
   "C:\Program Files\Common Files\QM\config\.keystore" -storepass
   C@labr1o -importcert -trustcacerts -alias <CA name> -file <CA
   name>.cer
   ```

   where <CA name> is the name of the certificate.

   Important: Always import the root certificate first.

4. Click Yes when the when the following prompt appears:

   ```
   Trust this certificate?
   ```

This prompt appears because the certificate is self-signed (that is, the certificate is issuer of the certificate is also the owner) and the keytool cannot follow the chain back to a trusted root CA.

Step 3: Import intermediate certificates into the Quality Management keystore.

Note: You can skip this step if the Quality Management certificate was signed by the root CA. If the Quality Management certificate was signed by an intermediate CA, then all intermediate certificates in the chain back to the root certificate must be imported.

From the command line on the Web Base server, enter the following command:

```
"C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
"C:\Program Files\Common Files\QM\config\.keystore" -storepass
C@labr1o -importcert -trustcacerts -alias <CA name> -file <CA
name>.cer
```

where <CA name> is the name of the certificate.

This command imports the intermediate certificates into the Quality Management keystore.

Step 4: Import the signed Quality Management certificate.

From the command line on the Web Base server, enter the following command:

```
"C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
"C:\Program Files\Common Files\QM\config\.keystore" -storepass
C@labr1o -importcert -alias jetty -file jetty.cer
```

This command imports the signed certificate into the Quality Management keystore.

Step 5: Restart the Jetty service.

On the Quality Management Web Base server, use the Windows Services utility in the Control Panel to restart the Jetty service.

Step 6: Import root and intermediate certificates into the client web browsers.

This step is not necessary in the following situations:

- The Quality Management certificate was signed by a well-known CA such as VeriSign, or Thawte. Most modern browsers come with the major commercial CA root certificates already installed. Lesser known CAs might not be installed.

- You are using Internet Explorer **and** an Active Directory CA where the Quality Management Web Base server and clients are all in the same Active Directory domain

To determine if you need to perform this step, start the client web browser and try to access Unified Workforce Optimization using the following URL:

```
https://<Web Base
server>/cwfo/apps/login.html?userLang=en&userTheme=
cisco&userCountry=
```

where <Web Base server> is the hostname or IP address of the server of the Quality Management Web Base server.

- If you can connect without errors or requests to install certificates, you do not have to perform this step.
- If you see a message indicating that the issuer of the certificate is not trusted, you need to perform this step.

Note: You must specify the same hostname or IP address specified for the Web Base server in System Setup Configuration (postinstall.exe). For example, if you specified a hostname in postinstall.exe, you must specify a hostname here.

Best Practices: Chrome provides more descriptive error messages when updating certificates. Use Chrome to troubleshoot certificate errors.

For more information about installing root and intermediate certificates on the desktop, see *Installing Root and Intermediate Certificates on Desktops*.

Expired Certificate from a Commercial Service

Your CA will assign an expiration date to the Quality Management certificate. When the Quality Management certificate expires you will need to create a new CSR and import it to replace the expired CSR. To replace an expired Quality Management certificate:

1. *Creating a Certificate Signing Request (CSR) for the Web Base Server*.
2. *Generating Certificates Using Commercial Services*.

To view the expiration date, double-click the Quality Management certificate or after the Quality Management is installed use the keytool -list command.

Certificates and Active Directory

You can generate signed Quality Management certificates using Active Directory Certificate Server (AD CS). AD CS is a CA.

When generating Active Directory certificates, remember the following points:

- The AD CS for the root domain generates its own self-signed certificate. The issuer and owner are the same. AD CS also signs the certificate for the intermediate certificate.
- A self-signed certificate is generated by Quality Management when it is installed. When a web browser encounters this certificate, it views the certificate as a security violation and generates an error.
- The intermediate AD CS signs the certificate for the Quality Management Web Base server and replaces the Web Base server IP address with its own domain name in the Issuer field.
- When all the certificates are signed, each certificate is linked to the previous certificate, with the final or root certificate included in the web browser's trusted root certificate store. This is known as a certificate chain. In this scenario, the web browser does not generate certificate errors.
- Root and intermediate certificates must be installed on both the Quality Management Web Base server and the web browser on each client machine.

Verifying the AD CS Supports the Subject Alternate Name (SAN) Certificate Feature

By default, the AD CS server does not allow the ability to add Subject Alternate Name (SAN) attribute to certificates. You need to enable this feature on you AD CS server.

> **Note:** Beginning with Google Chrome browser release 58, the Common Name is no longer used. If you are using Chrome as your browser, you **must** use the Subject Alternate Name (SAN) feature.

AD CS has policy modules that provide different services. The policy modules provide different types of extensions that can be enabled so clients can submit their requests for those features.

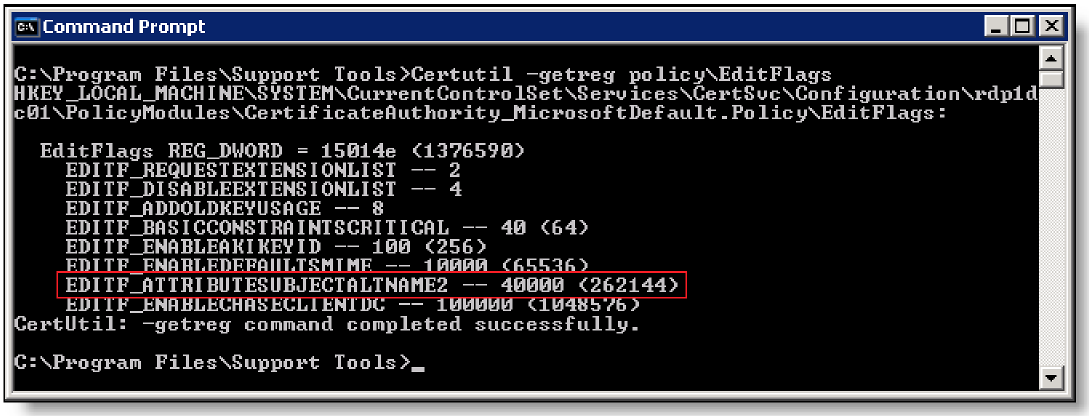
The CertificateAuthority_MicrosoftDefault.Policy is the default policy module on a Windows 2003 Certificate server. By default, it does not allow the ability to add SAN attributes to certificates.

Use the Certificate Database Tool to check the values of the Certificate Services registry keys and enable the SAN attribute:

1. From the command line on the Windows 2003 or 2008 Certificate server, go to the C:\Program Files\Support Tools directory and enter the following command:

   ```
   certutil -getreg policy\EditFlags
   ```

   The command lists the Certificate Services registry keys.



```
C:\Program Files\Support Tools>Certutil -getreg policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\rdp1d
c01\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

  EditFlags REG_DWORD = 15014e (1376590)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -getreg command completed successfully.

C:\Program Files\Support Tools>_
```

2. Verify that EDITF_ATTRIBUTESUBJECTALTNAME2 EditFlag is enabled.
3. If the EditFlag is not enabled, enter the following command:

```
certutil -setreg policy\EditFlags +EDITF_
ATTRIBUTESUBJECTALTNAME2
```

4. On a Windows 2008 Certificate server only, you need to enter these additional commands:

```
certutil -setreg policy\SubjectAltName enabled
certutil -setreg policy\SubjectAltName2 enabled
net stop certsvc
net start certsvc
```

For more information, go to the following topics on Microsoft website:

- Policy Modules: http://msdn.microsoft.com/en-us/library/aa387348%28v=vs.85%29.aspx.
- SAN certificate feature: http://techontip.wordpress.com/2011/06/06/how-to-make-sure-internal-certificate-authority-is-supporting-san-certificate-feature/

Generating Certificates Using Active Directory

Follow these steps to generate certificates using Active Directory Certificate Services (AD CS).

Step 1: Create a root CA signed certificate from AD CS.

1. Log in to the Active Directory server for the root AD CS.
2. From Internet Explorer on the Active Directory server, enter the following URL:

```
http://<myRoot>/certsrv
```

where <myRoot> is the root domain's IP address or hostname. The AD CS for this domain is the root for this network.

Example: `http://192.0.2.8/certsrv`

Note: You must specify the same hostname or IP address specified for the Active Directory server. For example, if you specified a hostname in the Active Directory server, you must specify a hostname here.

3. Click Download a CA Certificate, Certificate Chain, or CRL.
4. Select Base 64 encoded.

Note: Quality Management can only import Distinguished Base-64 encoded X.509 formatted certificates. These certificates have the following extension: CER.

5. Click Download the CA certificate and specify a descriptive name for the root certificate.

Example: `192.0.2.8_root_x509.cer`

See Microsoft Knowledge Base 555252 and *Expired Certificate from AD CS* for additional information.

Step 2: Download the intermediate certificates.

Note: You can skip this step if there are no intermediate certificates.

Perform this procedure for each intermediate certificate.

1. Log in to the Active Directory server for the intermediate AD CS.
2. From Internet Explorer on the Active Directory server, enter the following URL:

```
http://<myIntermediate>/certsrv
```

where <myIntermediate> is the intermediate domain's IP address or hostname. The AD CS for this domain where the Quality Management Web Base server.

Example: `http://192.0.2.21/certsrv`

Note: You must specify the same hostname or IP address specified for the intermediate domain. For example, if you specified a hostname in for the intermediate domain, you must specify a hostname here.

3. Click Download CA certificate, certificate chain, or CRL.
4. Click Download CA certificate and specify a descriptive name for the intermediate certificate.

Example: `192.0.2.21_intermediate-cert_x509.cer`

Step 3: Use the CSR to create a signed Quality Management certificate.

Note: This step requires that the EDITF_ATTRIBUTESUBJECTALTNAME2 EditFlag is enabled in the Certificate Services registry. See *Verifying the AD CS Supports the Subject Alternate Name (SAN) Certificate Feature* for instructions.

1. Log in to the Active Directory server for the intermediate AD CS.
2. From Internet Explorer on the Active Directory server, enter the following URL:

   ```
   http://<myIntermediate>/certsrv/
   ```

   where <myIntermediate> is the intermediate domain IP address or hostname. This is the domain where the Quality Management Web Base server resides.

Example: `http://192.0.2.8/certsrv`

Note: You must specify the same hostname or IP address specified for the intermediate domain. For example, if you specified a hostname in for the intermediate domain, you must specify a hostname here.

3. Click Request a Certificate.

Note: On some CA servers you might get an additional page where you must click Advanced Certificate Request.

4. Click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 File.
5. Open the CSR file that you created in Step 1 and copy the entire contents of the file into the Saved Request field, including the following lines:

```
----BEGIN NEW CERTIFICATE REQUEST----
----END NEW CERTIFICATE REQUEST
```

6. Select Web Server in the Certificate Template field.
7. To access the Quality Management Web Base server using an hostname or IP address, type the host

   name or IP address as a Subject Alternative Name (SAN) in the Attributes field. The format is as follows:

   ```
   SAN:DNS=<myDomain or IP address>
   ```

   where <myDomain or IP address> is the hostname or IP address.

Note: You must specify the same hostname or IP address specified for the Web Base server in postinstall.exe. For example, if you specified a hostname in postinstall.exe, you must specify a hostname here.

Note: If you want to more than one hostname or IP address, use an ampersand to separate each hostname or IP address.

Important: Once you specify a hostname as a SAN DNS attribute, you will lose the ability to connect to the Quality Management Web Base server using an IP address. If you try connecting to the Quality Management Web Base server using an IP address, you will receive a security error indicating a certificate mismatch. If you want to continue connecting to Quality Management Web Base server using an

IP address in Internet Explorer, you need to also add the IP address as a SAN DNS attribute to the Attributes field.

Example: `SAN:DNS=my.domain.com&DNS=192.0.2.0`

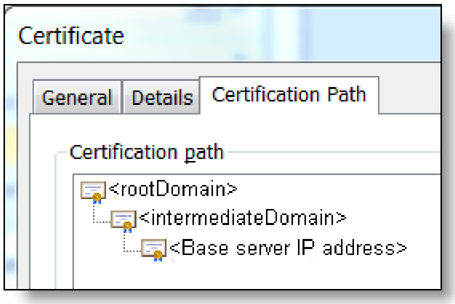
8. Click Submit.
9. Select Base 64 encoded and click Download certificate.

Note: Quality Management can only import Base-64 encoded X.509 formatted certificates. These certificates have the following extension: CER.

10. When prompted, provide a descriptive file name for the certificate.

Example: `jetty.csr`

11. Click Save As and specify where the file will be located.
12. Go to the location of the certificate and double-click the certificate file.
13. Select Certification Path tab, and verify the certification path is correct. It should include the IP address of the Quality Management Web Base server and the chain of certificates back to the root CA (see graphic).



If the certification path is not correct, download the root and intermediate certificates again from the correct AD CS domains.

If you added SAN attributes, click the Details tab and verify the SAN attributes are correct.

> **Note:** The AD CS will fail silently if the SAN attributes are not configured properly.

See *Expired Certificate from AD CS* for additional information.

Step 4: Import the root certificate into the Quality Management keystore.

1. Log in to the Quality Management Web Base server with administrator rights.
2. From the command line on the Web Base server, enter the following command:

   ```
   "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
   "C:\Program Files\Cisco\WFO_QM\Java\lib\security\cacerts" -
   storepass changeit -list -v
   ```

   This command lists the existing CA root certificates that comes bundled with QM Java. If your CA appears in this list, you do not have to proceed. If it is not in the list, continue to the next step.

3. Enter the following command:

   ```
   "C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
   "C:\Program Files\Common Files\QM\config\.keystore" -storepass
   C@labr1o -importcert -trustcacerts -alias <CA name> -file <CA
   name>.cer
   ```

   where <CA name> is the certificate file name.

   > **Important:** Always import the root certificate first.

   > **Example:** `"C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore "C:\Program Files\Common Files\QM\config\.keystore" -storepass C@labr1o -importcert -trustcacerts -alias 192.0.2.8_root_x509 -file 192.0.2.8_root_x509.cer`

4. Click Yes when the when the following prompt appears:

   ```
   Trust this certificate?
   ```

This prompt appears because the certificate is self-signed (that is, the certificate is also the owner) and the keytool cannot follow the chain back to a trusted root.

Step 5: Import intermediate certificates into the Quality Management keystore.

> **Note:** You can skip this step if the Quality Management certificate was signed by the root CA. If the Quality Management certificate was signed by an intermediate CA, then all intermediate certificates in the chain back to the root must be imported.

From the command line on the Quality Management Web Base server, enter the following command:

```
"C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
"C:\Program Files\Common Files\QM\config\.keystore" -storepass
C@labr1o -importcert -trustcacerts -alias <CA name> -file <CA
name>.cer
```

where <CA name> is the certificate file name.

Step 6: Import the Quality Management Jetty certificate into the Quality Management keystore.

From the command line on the Quality Management Web Base server, enter the following command:

```
"C:\Program Files\Cisco\WFO_QM\Java\bin\keytool.exe" -keystore
"C:\Program Files\Common Files\QM\config\.keystore" -storepass
C@labr1o -importcert -alias jetty -file jetty.cer
```

This command imports the signed Jetty certificate into the Quality Management keystore.

If the importation is successful, you will see the following message:

```
Certificate reply was installed in keystore.
```

Step 7: Restart the Jetty service.

On the Quality Management Web Base server, use the Windows Services utility in the Control Panel to restart the Jetty service.

Step 8: Import root and intermediate certificates into the client web browsers.

This step is not necessary in the following situations:

- The Quality Management certificate was signed by a well-known CA such as VeriSign, or Thawte. Most modern browsers come with the major commercial CA root certificates already installed. Lesser known CAs might not be installed.

- You are using Internet Explorer **and** an Active Directory CA where the Quality Management Web Base server and clients are all in the same Active Directory domain

To determine if you need to perform this step, start the client web browser and try to access Unified Workforce Optimization using the following URL:

```
https://<Web Base
server>/cwfo/apps/login.html?userLang=en&userTheme=
cisco&userCountry=
```

where <Quality Management server> is the hostname or IP address of the server of the Quality Management Web Base server.

- If you can connect without errors or requests to install certificates, you do not have to perform this step.
- If you see a message indicating that the issuer of the certificate is not trusted, you need to perform this step.

> **Best Practices:** Chrome provides more descriptive error messages when updating certificates. Use Chrome to troubleshoot certificate errors.

For more information about installing root and intermediate certificates on the desktop, see *Installing Root and Intermediate Certificates on Desktops*.

Expired Certificate from AD CS

Your CA will assign an expiration date to the Quality Management certificate. When the Quality Management certificate expires you will need to create a new CSR and import it to replace the expired CSR. To replace an expired Quality Management certificate, see *Creating a Certificate Signing Request (CSR) for the Web Base Server*.

To view the expiration date, double-click the Quality Management certificate or after the Quality Management is installed use the keytool -list command.

Installing Root and Intermediate Certificates on Desktops

To install the root on any intermediate certificates on a desktop:

1. Copy the root and any intermediate certificates to any location the client .

> **Note:** The root certificate must be installed first, and after that any intermediate certificates. Follow these steps for each certificate you want to install.

2. Double-click the certificate to open the Certificate dialog box.
3. On the General tab, click Install Certificate and then click Next.
4. Select the Place all certificates in the following store option, and then click Browse to select a certificate store:
   - For the root certificate, choose Trusted Root Certificate Authorities store
   - For intermediate certificates, choose Intermediate Certificate Authorities store
5. Click Next and then Finish. When asked if you want to install the certificate, click Yes.
6. Click OK after the certificate is installed.
7. Click OK to dismiss the dialog box.

To verify that the certificates where installed correctly:

Open Internet Explorer and enter the following URL:

```
https://<Web Base
server>/cwfo/aps/login.html?userLang=en&userTheme=
cisco&userCountry=
```

where <Web Base server> is the host name or IP address of the server that hosts the Quality Management Web Base Services.

If the certificates are correctly installed you should not see any security warnings. The URL contains HTTPS and a Lock icon appears in the Address bar.

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 Web Base Services.

The web page is ScreenRecordingThinClient.htm. It 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

To manually install the Recording Thin Client on a Citrix server:

1. Open the Citrix server's web browser and access the `Cisco Unified WFO Monitoring and Recording Thin Client.msi` file on the base server.

   ```
   http://<base server>/TUP/QM/ScreenRecordingThinClient.htm
   ```

   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 desktop.
3. Restart the Citrix server when prompted to ensure the services start correctly.

SNMP Integration

The following products include SNMP integration for their Monitoring and Notification (MANA) service.

- Cisco Quality Management 9.0, 10.0, or 10.5

MANA is responsible for sending notifications to administrators or supervisors when it detects events that might negatively affect the functioning of the software or system.

This document covers SNMP integration and how to take advantage of this method of notification when you install.

Definitions

The following table defines terms used in this document.

Term	Definition
MIB	Management Information Base. A defined hierarchy of data values managed by a single SNMP Agent application.
OID	Object Identifier. A unique string of digits representing a value defined in an MIB.
SNMP	Simple Network Management Protocol. A common network protocol that describes messages passed between SNMP-enabled applications.
SNMP Agent	An SNMP-enabled application that acts as a client to an SNMP management application by providing data values for registered OIDs.
SNMP GET	An SNMP message used to get a value for a particular OID.
SNMP Management Application	An SNMP-enabled application that can get or set information from a local or remote SNMP Agent application.
SNMP SET	An SNMP message used to set a value for a particular OID.
Trap	An unsolicited SNMP message sent from an SNMP agent to an SNMP management application.

SNMP Implementation

The MANA service already has methods to alert administrators of potential problems with Quality Management. These products extend this functionality to SNMP so that hardware/software management is provided for customers who already use SNMP management software.

The MANA service provides unsolicited alerts when it detects problem events. The alert contains the details of the problem, which enables action to be taken to prevent loss of software functionality. The SNMP trap message contains the same information and can be sent out to multiple SNMP management stations.

MIBs

Two MIBs are used to define the trap messages sent by the Quality Management software:

- The SMI MIB contains definitions of frequently-used objects
- The GENERIC-TRAP MIB file defines the trap message format

Whereas most MIBs are very specific in their use and definitions, the Generic Trap MIB was designed to define a generic message that can be sent by any Cisco application. The data values contained in the trap are used to decode the trap's contents.

For example, these OIDs are used to specify a particular Cisco product:

- 1.3.6.1.4.1.29988.1.1.1—used only for Quality Management
- 1.3.6.1.4.1.29988.1.1.2—used only for Cisco Agent Desktop
- 1.3.6.1.4.1.29988.1.1.3—used only for Cisco Workforce Management

Rather than use these very specific OIDs, the Generic Trap MIB uses this single OID:

- 1.3.6.1.4.1.29988.1.2—uses a variable that maps to the appropriate product name

Using MIBs

The *Installation Guide* and *Administrator Guide* for Quality Management explain how to install the product software and configure it to enable the sending of SNMP traps. Once configured, MANA will send the SNMP trap messages to all the IP addresses configured. These IP addresses represent machines that are running some type of SNMP management software.

The MIB files are used in order for the management software to display the information from a Ciscogeneric trap in a readable format, or to allow decision code running on the management station to interpret these traps.

The two Cisco MIBs describe the layout of information found in the Cisco trap in a language that SNMP management stations understand. The MIB files need to be placed on a drive accessible to the SNMP management software. Once there, the administrator configures the management station to load the MIB files. How this is done varies, based on the SNMP management station software provider.

The SNMP error codes are the same as the MANA error codes. These error codes are documented in the *Error Code Dictionary* for version 8.6 or later.

Generic Trap

The trap message defined in the GENERIC-TRAP MIB is a set of string and numeric values that define the event. The OIDs, field names, and field descriptions are shown in the table below.

OID	Field	Description
1.3.6.1.4.1.29988.1.1	cigtTimestamp	Numeric. The date and time the event was generated. Number of seconds since 1/1/1970.
1.3.6.1.4.1.29988.1.2	cigtProduct	String. The name of the product sending the trap.
1.3.6.1.4.1.29988.1.3	cigtVersion	String. The version of Quality Management that is installed.
1.3.6.1.4.1.29988.1.4	cigtModule	String. The Quality Management module reporting the event. For Quality Management, this is MANA. In the future, other modules might be used in addition to MANA.
1.3.6.1.4.1.29988.1.5	cigtSeverity	Numeric. The severity of the event. ■ 1 = Informational. Normal processing messages. ■ 2 = Warning. Abnormal event that does not affect product functionality. ■ 3 = Error. Error that affects some product functionality. ■ 4 = Fatal. Serious error that causes loss of basic functionality.
1.3.6.1.4.1.29988.1.6	cigtEventCode	String. An alphanumeric error code representing the event. This code is used to look up additional information in the *Error Code Dictionary*.
1.3.6.1.4.1.29988.1.7	cigtEventText	String. A readable string describing the event.

Deploying Applications on the Desktop

This section describes how to install and upgrade desktop applications for .

You can use one of the following options to install the desktop applications on desktops:

- Manual installation
- Administered installation—using one of the automated package distribution tools.

For best practices, see *Windows Installer Logging*.

Windows Installer Logging

Best Practices: Enable Windows Installer logging to capture loggable issues when installing desktop applications.

Windows Installer logging can be enabled. This ensures that any loggable issues are captured efficiently. To enable Windows Installer logging, run installations using the following command:

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

where <client installation executable> is the name of the desktop application's executable file and <logfile path and name> is the name and location of the log file. The <logfile path and name> is optional. If you do not provide a name and location for the log file, the log file will be saved to a temp folder.

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

Note: Specify a location for the logfile path and name where you have write permission.

Client Installation Packages Locations

On a successfully installed production server, Microsoft Installer (MSI) packages are located at:

- Quality Management: http://<Web Base server>/TUP/QM/Administrator.htm

An MSI package is intended for both manual and automated deployment.

You can also generate MSI packages using a client configuration tool and unconfigured installation templates. The client configuration tool is located at:

- Quality Management: `C:\Program Files\Cisco\WFO_QM\bin\ConfigureClients.exe`

The installation ISO contains unconfigured installation templates that, with the use of a client configuration tool, can be configured so that desktop 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 ISO:

- Quality Management Clients:
  - Admin
  - Recording
  - RecordingThinClient

Manual Installation

The following topics describes how to deploy desktop applications manually.

Manual Installation Requirements

When installing desktop applications manually, note the following requirements:

- Machine Policy Value for EnableUserControl—the machine policy value for EnableUserControl must be set to either Not Configured or Enabled. If it is set to Disabled, you will not be able to install any desktop applications on the client machine.
- Elevated Privileges Policy for Windows Installer Installation—to allow users with limited privileges to install a desktop application 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.

  To elevate the privileges on a user’s computer so the user can install the desktop applications:

  1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
  2. Right-click the appropriate organizational unit (OU) and 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. Choose 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. Choose Set to Enabled, and then click OK.

   You must enable this GPO under both the User Configuration and Computer Configuration sections for it to take effect.

Installing Desktop Applications

You can install the desktop applications from web pages that reside on the Web Base server. These web pages are created when you install the Base Services.

Install the desktop applications after you install and configure the services for Recording and Quality Management.

To install desktop applications for Recording and Quality Management:

1. On 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. Your options are as follows:

   ■
   - http://<Web Base server>/TUP/QM/Administrator.htm—contains links to the install files for all desktop applications—Quality Management Administrator and Desktop Recording service, and Cisco Screen Player Plug-in.

     Note: Quality Management Administrator is automatically installed on the Web Base server.

   - http://<Web Base server>/TUP/QM/Recording.htm—contains a link to the

Desktop Recording service install files.

- http://<Web Base server>/TUP/QM/MSPackage.htm—contains a link to the Microsoft Visual C++ 2013 Redistributable Package (x86) install file. The Microsoft Visual C++ 2013 Redistributable Package is only required for managers and supervisors that want to use the Live Screen Monitoring feature.

  Customers whose IE browser permission level blocks their browser from downloading the ScreenViewer.cab file should download this file:

  ```
  <INSTALLDIR>WFO_QM\Jetty\webapps\TUP\QM\Cisco Monitoring and
  Recording Screen Viewer.msi
  ```

  After the installer is downloaded, it can be pushed to the affected desktops.

The installation web page appears.

3. Follow the instructions on the web page to install the desktop application.
4. Choose the option that applies to this installation:

   - The following message appears when installing the Desktop Recording Service or the Recording Thin Client:

     ```
     You must restart your system for the configuration changes to
     Cisco Monitoring and Recording Recording to take effect. Click
     Yes to restart now or No if you plan to restart later.
     ```

     > **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.

   - If the previous option does not apply, no additional action is required.

Administered Installation

The following topics describe how to deploy desktop applications automatically.

Administered Installation Requirements

The requirements for an administered configuration are as follows:

- Execution—Installations must be executed on the target machine.
- Per-machine vs. per user—Installations must be deployed on a per-machine basis. Per-user installations are not supported.

Using Automated Package Distribution Tools

You can deploy (push) executable-based desktop application installations through automated package distribution tools that make use of the Microsoft Windows Installer service.

Administered Installation Best Practices

Create a deployment package for each installation package.

Before deploying an installation package, the deployment engineer should test an installation and an uninstallation of the deployment package.

> **Best Practice:** Deploy each installation package using its own deployment package. Using separate deployment packages allows you to isolate potential issues faster than a composite 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. Verify that the required hardware and software are installed on the desktop clients. See the Desktop Requirements for more information.
3. Install the servers to obtain valid client installation packages or use the client configuration tool. See *Client Installation Packages Locations* for the location of the client installation packages on the server.
4. Manually deploy client installation packages to ensure that the installs are compatible with your environment.

   This will isolate product installation vs. automated deployment issues.
5. Create your deployment packages in accordance with the requirements listed in Administered Installation Requirements.

   > **Note:** Cisco recommends creating installation and uninstallation deployment packages.

6. Test the deployment packages.
7. 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.

Configuring Desktop Installation Files

To configure client installation files with the client configuration tool (ConfigureClients.exe for Recording and Quality Management):

1. Create a virtual drive and then load the ISO on that drive.
2. Copy the Clients folder and all of its contents from the Quality Management installation ISO to a desktop.
3. On the desktop, open a command window and navigate to the Clients folder.
4. Run the ConfigureClients.exe as administrator.
5. The configuration tool starts.
6. Type the IP address or hostname of the Web Base server and press Enter.
7. Type the IP address or hostname of the Surrogate Host and press Enter.

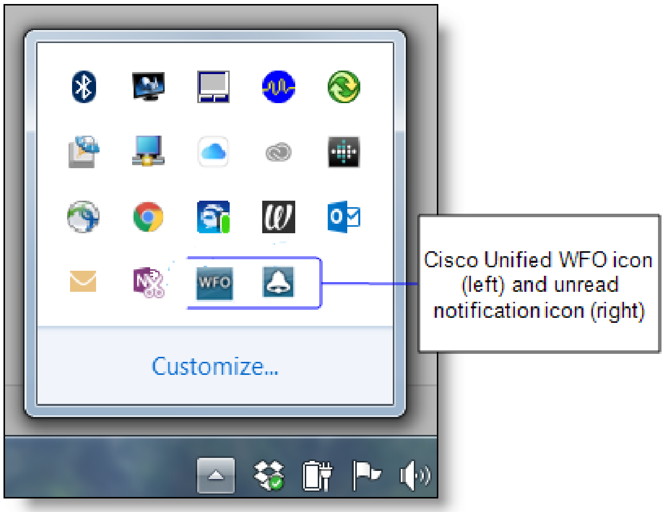
   The utility creates installation files for all Quality Management desktop applications.

Installing the Unified Workforce Optimization Notification Client

The Unified Workforce Optimization Notification client can be used in systems that use Active Directory logins to access Unified Workforce Optimization. This feature is not available in systems that do not use Active Directory logins.

When this client is installed on the user’s desktop, any notifications and alerts that the user receives via the Alerts bubble on the Unified Workforce Optimization menu bar are also displayed as toaster popups on the desktop. An icon for Unified Workforce Optimization is present in the system tray, as well as an icon that appears whenever an unread notification is present.

Alerts and notifications are displayed whether or not the user is logged into Unified Workforce Optimization. See the *Recording and Quality Management User Guide* for more information on using the system tray icons.


WFO
Customize...
Cisco Unified WFO icon (left) and unread notification icon (right)

The Notification client can be installed manually on each user's PC, or automatically by a system-wide push. The installation file is accessed from a web page located on the Base services server.

Manual Installation

To install the Notification client manually, follow these steps.

1. On the PC where you want to install the Notification client, start the browser.
2. Navigate to this URL:

   ```
   http://<Base services server IP address>/TUP/QM/Notification.htm
   ```

3. Follow the instructions on the page.

> **Note**: You must have Administrator privileges on the PC in order to download and install the Notification client. If User Account Control (UAC) is off, you will not be able to download and install the client. If UAC is on, you will be asked to provide the Administrator credentials and then you can proceed with the installation. Alternatively, an administrator can configure the elevated privileges policy so that users with limited privileges can install a desktop application. For more information, see *Manual Installation*.

Automated Installation

The Notification client MSI-based installation can be deployed ("pushed") via a third-party automated package distribution tool that makes use of the Microsoft Windows Installer service. See *Administered Installation* for more information.

Configuring the Notification Client Installation File

Run the Notification Client Configuration tool (ConfigureNotificationClient.exe) to create the installation file for the Notification client.

1. Create a virtual drive and load the QM installation ISO on that drive.
2. Copy the Clients folder and all its contents from the QM installation ISO to a desktop.
3. On the desktop, open a command window and navigate to the Clients folder.
4. Run ConfigureNotificationClient.exe as an administrator.
5. After the tool starts, follow the prompts. Enter the IP address or host name of the Surrogate Host and press Enter.

   The utility creates the Notification Client installation file.

Managing Certificates

How you manage certificates on a desktop depend on where the certificate is signed.

If your signed certificate is from a well known Certificate Authority (CA) or you imported the signed certificate into Active Directory, there is nothing additional that you need to do. Well known CAs, like VeriSign or Thawte, include certificates as part of the Java cacerts store.

If your signed certificate is from Active Directory Certificate Server (AD CS), and you imported the signed certificate into Active Directory, there is nothing additional that you need to do. If the desktop client is not included in the Active directory domain, you need to import the certificate.

Lesser known CAs, such as GoDaddy, will need to be installed on the client machine or browser. You can add a trusted root CA to a Group Policy object (GPO). Microsoft provides instructions for adding a trusted root CA to a GPO at http://technet.microsoft.com/en-us/library/cc738131.aspx.

Internet Explorer will look for the certificate in the internal machine certificate store on the desktop.

Upgrading the Desktop Applications

To upgrade Recording and Quality Management desktop applications:

1. If you are upgrading from 11.0 or earlier, uninstall the Cisco Screen Player Plug-in.

   > **Note:** The Cisco Screen Player Plug-in is no longer required with versions 11.0or later.

2. Choose one of the following upgrade options:

- If you are upgrading from a version prior to 11.0, you must uninstall the existing desktop applications before you install 11.5.

  > **Important:** Over-the-top upgrades from versions prior to 11.0 are not supported and will be blocked.

- If you installing version 11.0 or later, you can install the desktop applications over-the-top.

3. Install the following applications onto each desktop:
   - Cisco Screen Player Plug-in
   - Desktop Recording service
   - Quality Management Administrator—on the administrator’s machine only

See *Installing Desktop Applications* for more instructions.

Testing the Desktop Recording Service Installation on Desktops

If you have desktops that run on different operating systems, test three or four desktops for each operating system using Recording and Quality Management in your environment and generate test calls to phones associated with each of the desktops before a scheduled upload occurs.

> **Example:** You environment includes desktops with administrative privileges and laptops with administrator privileges.

To test Desktop Recording Services after a fresh installation or an upgrade:

1. Log on to a 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 desktop in your test set.
5. After testing the sample desktops, continue updating the remaining desktops.

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

Removing Quality Management

To uninstall Quality Management, you must proceed in the following order:

- Uninstall any ET present.
- Uninstall the Quality Management services.

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.

When you uninstall Quality Management, Zeranoe FFmpeg (FFMPEG.exe) is automatically uninstalled.

Best Practices: If your reinstall Quality Management, you must also reinstall Zeranoe FFmpeg. See *Zeranoe FFmpeg* for more information.

Removing Services

When you remove Quality Management services, the Quality Management software is completely removed except for the Quality Management database. The components can be removed in any order.

To remove Quality Management services, follow these steps:

1. Log into the Quality Management server as the local machine administrator or domain administrator.
2. Start the Programs and Features utility in Control Panel.

   There can be up to three programs listed for Quality Management, depending on what you installed on the server:

   a. Cisco Monitoring and Recording Services Framework

   b. Cisco Monitoring and Recording Services

   c. Cisco Monitoring and Recording Services Jetty

   If you choose (a) for removal, (b) and, if present, (c) are also removed. If you choose either (b) or (c) for removal, only that program is removed.

3. Click Uninstall, and follow the prompts.

4. After the uninstall is completed, you are prompted to reboot. You are given the option to reboot now or later. It is recommended that you reboot immediately to complete the uninstallation process.

Removing a Quality Management Desktop Application

To uninstall the components identified in Removing Quality Management :

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.

   If you are running Windows 7, a Reboot Warning dialog box might appear behind the current window after you uninstall 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.

   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.

   Windows removes the application.

4. Restart the machine.

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:

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.

   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 the custom configuration files on your system.

- Upgrading your system to the latest version of Quality Management.
- Making a disaster recovery backup for your custom configuration files.

The data that you should back up includes the Quality Management database, the .keystore file if you are using signed certificates, and your custom logo.

Quality Management Database Disaster Recovery

The SQMDB database stores historical data and report data. Cisco recommends backing up the SQMDB database periodically for the purpose of database disaster recovery.

> **Best Practices:** Always back up the SQMDB database before an upgrade. This allows you to roll back to the previous version, if necessary.

Back up the SQMDB database to another folder on the computer that hosts the Microsoft SQL Server.

To back up your Quality Management database:

- Back up the SQMDB database to another folder on the computer that hosts the Microsoft SQL Server.

To restore your Quality Management database:

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 Web Base server
- MediaSense Subscription service

3. Restore the original SQMDB database on the computer that host the Microsoft SQL server.
4. Restart the services for Quality Management you stopped in Step 2.

Jetty SSL Certificate File Recovery

To back up the .keystore file:

1. On the Web Base server where the .keystore file resides, go to the following directory:

   C:\Program Files\Common Files\QM\config\

2. Copy the .keystore file and save it to a safe location.

To restore the .keystore file:

1. Go to the location where the backup .keystore file resides and copy the .keystore file.
2. On the Web Base server, paste the .keystore file in the following directory:

   C:\Program Files\Common Files\QM\config\

Custom Logo File Recovery

To back up your custom logo:

1. Navigate to the C:\Program Files\Cisco\WFO_QM\Jetty\report_solutions\reports folder.
2. Copy the logo file and save it to a backup folder.

To restore your custom logo:

1. Start postinstall.exe or Quality Management Administrator.
2. On the Enterprise Settings window, click Report Logo Configuration.
3. Click Select New Logo, browse to the location of your logo, and then click Select Image.
4. Click Save.
5. Restart the Jetty service.