



## **Cisco Unified Workforce Optimization**

Quality Management Installation Guide 2.6  
September 2008

### **Americas Headquarters**

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

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

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

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

*Quality Management Installation Guide*

© 2008 Cisco Systems, Inc. All rights reserved.

© 2008 Calabrio, Inc. All rights reserved.

---

# Contents

---

## Overview 7

- Introduction 7
  - What's New in This Version 7
- QM 2.6 Components 9
  - Client Applications 9
  - Services 9
- System Configuration 11
- System Requirements 13
  - System Environment 13
  - Data Configuration Environment 13
  - Operating Environment 13
  - Server Capacity Guidelines 14
  - Sizing Guidelines 14
  - Remote Agent Requirements 14
  - Supported IP Phones 15
  - Supported Cisco Unified Outbound Dialer Modes 16
  - Required Third Party Applications 16
- Firewall Requirements 18
- QM Desktop Recording Requirements 19
  - Required Phone Device Parameters 19
  - Required Codecs 19
  - Hard Drive Space on Agent Computers 19
  - QM Desktop Recording and Network Interface Cards 20
  - QM Desktop Recording Phone Configurations 21

---

## Installing QM 23

- Introduction 23
- Prerequisites 24
  - Install Microsoft SQL Server 2005 24
  - Configure SQL Server 2005 for QM 25

---

# Contents

- Add Windows Firewall Exclusions 25
- Allow Remote Connections 26
- Configure the SQL Server Browser 26
- Install Windows SNMP Services 27
- Installing QM Services 28
- QM Configuration Setup 30
  - Entering Configuration Data in Initial Mode 31
  - QM Configuration Setup Steps 33
    - Cisco Unified CC Database 33
    - Cisco Unified CM 35
    - QM Databases 37
    - QM CTI Service 39
    - Enterprise Settings 40
    - Recording File Storage Location 45
    - Upload Settings 47
    - Monitoring and Notification 49
    - Status 62
  - Entering Configuration Data in Update Mode 62
- Configuring Proxy Gateway 64
- QM Configuration Setup Tools 66
  - Start Local QM Services 67
  - Create Database Catalogs 67
  - Generate Info for MSI Clients 67
  - Download/Install JTAPI 67
  - Encrypt Audio Files 67
  - Set Recording Home Directory 68
  - Generate SSL Certificate 68
  - Test CTI Service(s) 68
  - Display Metadata Encryption Key 68
  - Choose Monitor Adaptor 68
  - Remove Server-Based Recording Service 69
- Upgrading from Previous Versions 70
- Setting Up NT Authentication for the Cisco Unified CC Database 71
  - Set Up NT Users 71

---

## Contents

- Configure the QM Sync Service 72
- Verify the Connection 72
- Setting Up Named Pipes for the Cisco Unified CC Database 74
- Installing QM Desktop Applications 76
  - Overview 76
  - Enabling the Elevated Privileges Policy for Windows Installer Installations 76
  - Installation Procedure 77
- Using Automated Package Distribution Tools 78
  - Requirements 78
    - Execution 78
    - Per-Machine vs. Per-User Installation 78
    - Privileges 78
    - Automated Package Installation vs. Manual Installation 78
    - Multiple Software Releases 79
    - Reboots 79
  - Best Practices 79
    - Windows Installer Logging 79
    - Deployment 80
      - Installation and Uninstallation Deployment Packages 80
  - Recommended Deployment Preparation Model 80
  - Client Installation Packages on the Installation CD 80

---

### Removing QM 83

- Removing QM 83

---

### Index 87

---

## Contents

---

# Overview

# 1

---

## Introduction

Quality Management (QM) 2.6 is installed in this order:

1. Prepare servers for QM installation
2. Install and configure QM services on each server component
3. Install QM Administrator to configure users, groups, workflows, and other QM elements
4. Install QM Recording on client PCs
5. Install QM Desktop on appropriate users' PCs

## What's New in This Version

Quality Management 2.6 includes the following new features:

- Recording supported for Cisco Mobile Agents, thin client agents, and agents who use phones without PCs
- Recording supported for PCs with Microsoft Windows Vista
- Support for dual-monitor recording
- QM Desktop recordings tab/playback optimized for the 4:3 and 16:9 aspect ratios
- Voice and screen recordings can now be exported in Windows Media Video (WMV) format
- Voice recordings can now be exported in Windows Media Audio (WMA) format in addition to WAV format
- Supervisor evaluation approval
- Save in-progress evaluations
- Support for the G.722 codec
- Session timeouts for desktop clients and reports

- Archiving at the team level
- Compatibility with Cisco Unified Contact Center Express 7.0
- Login authentication using Active Directory 2008
- Playback of all segments of a call that is transferred through the contact center
- APIs for the following:
  - Export a recording based on its ID or metadata
  - Search for a recording
  - Edit metadata associated with a recording
  - Delete a recording
  - Pause voice and screen recording
  - Client-side recording controls

## QM 2.6 Components

---

The following client applications and services make up the QM system.

### Client Applications

The QM client applications are installed from web pages created on the Base Services server.

#### **QM Administrator**

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

#### **QM Desktop**

QM Desktop is used by evaluators to score contacts, by agents, supervisors, and managers to view evaluated contacts and reports, and by archive users to access archived contacts. Each user role has a different level of access to information.

#### **QM Recording**

QM Recording, located on the agent PC, is responsible for recording contacts and collecting metadata associated with recorded calls. The recordings are uploaded to the Voice and Screen servers and the metadata is uploaded to the QM database.

### Services

The QM services are installed from the QM CD.

#### **Quality Management CTI Service**

The QM CTI service acts as a bridge between the QM Recording service and the Cisco Unified Communications Manager/CTI Manager. It sends events to the QM Recording service when the status of monitored phones changes.

#### **Quality Management DB Cleaner Service**

The DB Cleaner service purges records from the QM database and media files from the Voice and Screen servers on a daily basis according to the retention times configured in QM Administrator.

#### **Quality Management DB Proxy Service**

The DB Proxy service is the single point of connection between users and the QM database.

#### **Quality Management Desktop Recording Service**

The Desktop Recording service is the end-point utility that enables the recording of agent contacts. It is resident on the agent's PC.

#### **LDAP**

LDAP contains information about the system's users, organizations, configuration, and workflow. It supplies information about agents and their workflows to the QM Recording service.

**Quality Management LDAP Monitor Service**

The LDAP Monitor service constantly checks LDAP to ensure that it is running. If LDAP stops, the LDAP Monitor service restarts it.

**Quality Management Monitoring and Notification (Mana) Service**

The Monitoring and Notification service monitors the QM system in real time and notifies administrators via event viewer or email when problems occur. The problems that trigger notification are selected in QM Administrator.

**Quality Management Monitor Service**

The Monitor service works in conjunction with the Network Recording service. It captures the packets that the Network Recording service records.

**Quality Management Network Recording Service**

The Network Recording service enables recording for agents who are configured for server-based recording.

**Quality Management Sync Service**

The Sync service reads data every 10 minutes from the ACD and synchronizes that information with QM.

**Quality Management Tomcat Service**

The Tomcat service webserver hosts the QM Reports engine, File Transfer Servlet (FTS), Server API engine, and Licensing engine.

**Quality Management Upload Controller Service**

The Upload Controller manages the uploading of recordings and recording metadata to the Voice and Screen servers.

## System Configuration

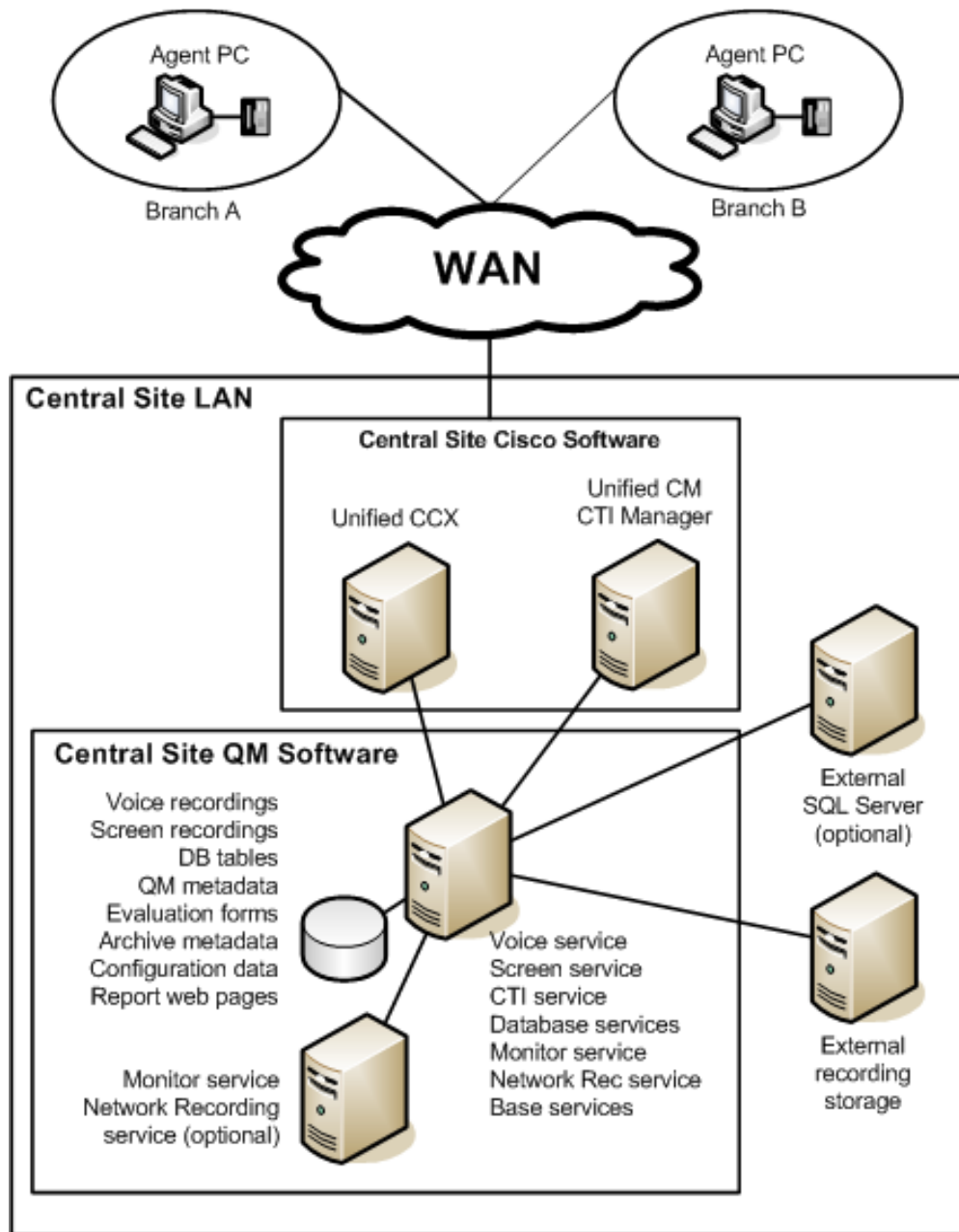
---

One system configuration is supported. This configuration is able to use an external storage server to store/archive voice and screen recording files (see "[Set Recording Home Directory](#)" on page 68). The supported configuration is illustrated in [Figure 1](#).

**NOTE:** A single deployment supports either the Basic bundle of QM or the Advanced bundle of QM, but not both.

**NOTE:** To maximize QM's performance and data storage capacity, it is strongly recommended that no other applications reside on the servers that host the QM services.

Figure 1. Supported configuration



## System Requirements

### System Environment

QM 2.6 is integrated into the following Cisco Unified Contact Center Express (Unified CCX) environment:

Table 1. System environment

ACD	Cisco Unified Communications Manager
Unified CCX 7.0	6.1, 7.0

### Data Configuration Environment

System configuration data is maintained using the following:

- Directory Services—OpenLDAP v2.2.17
- Microsoft SQL Server 2005 (Processor Licensing)

### Operating Environment

QM 2.6 runs in the operating environment described in [Table 2](#) and [Table 3](#).

Table 2. Supported desktop component operating systems and hardware

Operating System	Minimum Hardware Requirements		
	QM Administrator QM Desktop	QM Recording Basic Bundle	QM Recording Advanced Bundle
Windows XP Professional, Service Pack 3 or later	1 GHz processor 256 MB RAM 200 MB free space 100+ MB NIC*	500 MHz processor 256 MB RAM 1 GB free space 100+ MB NIC*	2 GHz processor 2 GB RAM 1 GB free space 100+ MB NIC*
Windows Vista Business, Enterprise, and Ultimate Editions	1 GHz processor 256 MB RAM 200 MB free space 100+ MB NIC*	1 GHz processor 1 GB RAM 1 GB free space 100+ MB NIC*	2 GHz processor 2 GB RAM 1 GB free space 100+ MB NIC*

\* NICs must support Promiscuous Mode. For a list of supported NICs, see *Network Interface Cards (NICs) Tested with Cisco Agent Desktop (CAD) and CTI Toolkit Desktop Silent Monitor—Reference Information* available at [http://www.cisco.com/en/US/prod/voicesw/custcosw/ps5693/ps14/prod\\_system\\_requirements0900aecd800e3149.pdf](http://www.cisco.com/en/US/prod/voicesw/custcosw/ps5693/ps14/prod_system_requirements0900aecd800e3149.pdf)

Table 3. Supported QM central server operating systems and hardware

Operating System	Minimum Hardware Requirements
Windows 2003 Server Service Pack 2 5 Client Access Licenses (CAL)	Cisco Media Convergence Server (MCS) platform or exact equivalent. For a list of supported MCS-equivalent platforms see <a href="http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html">http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html</a>

### Server Capacity Guidelines

Use the capacity guidelines in Table 4 to determine what MCS server or MCS server equivalent to use as the QM central server.

Table 4. QM central server capacity guidelines

Single Server Hardware	Maximum Number of Named Users	Maximum Number of Concurrent Agents
MCS-7816	450	150
MCS-7825	900	300
MCS-7835	1500	300
MCS-7845	3600	300

### Sizing Guidelines

In order to estimate the amount of disk storage required for your system, use the following guidelines:

- Screen recordings: ~1.2 MB per minute of recording
- Voice recordings: ~120 KB per minute of recording

### Remote Agent Requirements

Agents who do not work onsite are supported in these situations:

- They connect to the network via a Cisco 831 or 871 router and use a supported IP phone
- They use Cisco Remote Agent and are configured for server-based recording

## Supported IP Phones

All phones used by QM must support endpoint monitoring. [Table 5](#) is a list of supported IP phones.

Table 5. Supported IP phones

Phone Model	Protocol	PC Port	Unified Communication Manager	
			4.3	7.0
7910	SCCP	x	x	x
7911	SCCP	x	x	x
	SIP	x		x
7931	SCCP	x		x
7937	SCCP	x		x
7940	SCCP	x	x	x
	SIP	x		x
7941	SCCP	x	x	x
	SIP	x		x
7941G-GE	SCCP	x	x	x
	SIP	x		x
7942	SCCP	x		x
	SIP	x		x
7945	SCCP	x		x
	SIP	x		x
7960	SCCP	x	x	x
	SIP	x		x
7961	SCCP	x	x	x
	SIP	x		x
7961G-GE	SCCP	x	x	x
	SIP	x		x
7962	SCCP	x		x
	SIP			x

Table 5. Supported IP phones — *Continued*

Phone Model	Protocol	PC Port	Unified Communication Manager	
			4.3	7.0
7965	SCCP	x		x
	SIP			x
7970	SCCP	x	x	x
	SIP	x		x
7971	SCCP	x	x	x
	SIP	x		x
7975	SCCP	x		x
	SIP	x		x
7985	SCCP	x	x	x
IP Communicator	SCCP		x	x
	SIP			x

### Supported Cisco Unified Outbound Dialer Modes

QM 2.6 supports the Direct Preview dialing mode.

### Required Third Party Applications

QM 2.6 requires the following third party applications in order to run successfully:

Table 6. Required third party applications

Application	Installed Where	Use
Microsoft Internet Explorer 6 or 7	QM Desktop	HTML-based reports
Adobe Acrobat Reader 6.0 or later	QM Desktop	PDF-based reports and QM user documentation. Free download at <a href="http://www.adobe.com">www.adobe.com</a>
Microsoft SQL Server 2005	QM Database server or offboard server	Database
Apache Tomcat 5.5.9	QM Base server QM Voice server QM Screen server	Reports, recording uploads, licensing

Table 6. Required third party applications – *Continued*

Application	Installed Where	Use
Java Runtime Environment (JRE) 1.5.0 update 15 with timezone update tzdata2008c applied	All QM components	Provides an environment in which Java applications can be executed
Proxy Networks Proxy/Screen Recording 6.0	QM Desktops	Screen recording

## Firewall Requirements

For QM to function correctly, the ports in [Table 7](#) must be opened in the Windows Firewall. If the Windows Firewall is used and in operation when QM is installed, the QM installation process opens all ports and programs as needed except those for the Microsoft SQL Server (by default, 1433 and 1434).

If another firewall is used, or if you turn on the Windows Firewall after QM is installed, these ports must be opened manually. See your firewall documentation for instructions.

Table 7. QM Port Usage

Port/Program	Type	Description
7	TCP	Ping port
2303	UDP	Proxy Network port
8088	TCP	Tomcat port
8448	TCP	Tomcat SSL port
38983	TCP	LDAP port
52102	TCP	CTI port
52103	TCP	DB Proxy port
59011	TCP	Sync port
59100	TCP	Controller port
59101	TCP	Monitor server port
59102	TCP	Recording server port
59500-59900	UDP	Recording server ports
RecordServer.exe	TCP	Recording server

## QM Desktop Recording Requirements

This section applies to client desktop (endpoint) recording.

### Required Phone Device Parameters

For QM Desktop Recording to function correctly, several phone device parameters in Cisco Unified CM Administration must be enabled. They are enabled by default. If for some reason they have been disabled, follow this procedure to re-enable them.

#### *To re-enable the phone device parameters:*

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

The phone device's Phone Configuration page appears.

2. In the Product Specific Configuration Layout section, set these parameters to Enabled:

- PC Port
- PC Voice VLAN Access
- Span to PC Port

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

3. Click Update.

### Required Codecs

QM supports the G.711, G.722, and G.729 codecs. QM Desktop Recording (endpoint recording) and QM Network Recording (server-based recording) will not function correctly if IP phones use any other codec.

Consult the Cisco Unified CM documentation for information on changing a phone device's codec.

### Hard Drive Space on Agent Computers

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

- Voice recordings: 100 MB
- Screen recordings: 250 MB

Once space is freed up, recordings will resume.

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

## QM Desktop Recording and Network Interface Cards

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

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

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

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

The IP phone's VLAN ID can be obtained from the phone's Network Configuration screen (press Settings and then choose Network Configuration). See the documentation specific to your version of Cisco Unified Communications Manager and IP phone model for more information.

The following is a partial list of supported NICs.

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

## QM Desktop Recording Phone Configurations

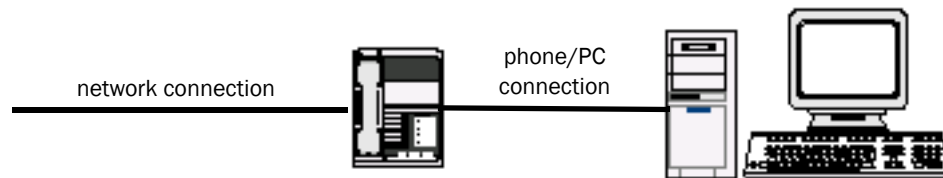
Two phone configurations for endpoint recording are supported:

- Hard IP phone and agent computer daisy-chained to the network ([Figure 2](#)). Multiple daisy-chained phones are not supported.
- Cisco IP Communicator soft phone on the agent's computer, connected to the network ([Figure 3](#)). No hard IP phone can be on the same network connection as the agent PC. Cisco IP Communicator must be in the computer's startup menu so that it is detected by QM Desktop Recording.

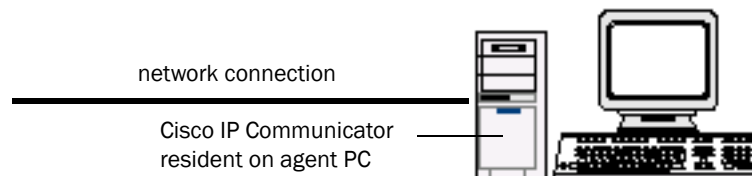
**NOTE:** Shared lines are not supported.

**NOTE:** Information about configuring phones for server-based recording can be found in the document *Configuring and Maintaining VoIP Monitoring and Recording*.

**Figure 2.** QM recording hardware setup (hard IP phone)



**Figure 3.** QM recording hardware setup (Cisco IP Communicator soft phone)





---

## Introduction

---

QM is installed in this order:

1. Install QM services
2. Run QM Configuration Setup on the Base Services server, and then on the other QM service servers
3. Install QM client applications

The QM services are installed from the QM CD. The QM client applications are installed from either the QM CD or from a web page located on the QM Base Services server.

## Prerequisites

---

Before you install the QM services, you must install Microsoft SQL Server 2005, either co-resident with the QM Database service or on an off-board server, and configure it for QM.

### Install Microsoft SQL Server 2005

Install Microsoft SQL Server 2005 and the following components as per the SQL Server documentation:

- SQL Server Database Services
- Workstation components, Books Online, and development tools

**NOTE:** The SQL Server installation installs the SQL Browser Service. By default, this service is set to be started manually, not automatically. If you are using an instance name and not the default instance, you must set the SQL Browser Service to start automatically.

Once the Microsoft SQL Server 2005 and the components are installed, create a Login User and assign a username and password.

**NOTE:** You will need the DBinstance name, username and password created here to complete the QM Database window in QM Configuration Setup, which runs automatically after you install the QM services.

**NOTE:** SQL Server must be set up with case-insensitivity (SQL collation name Latin1\_General, which is the default setting. See <http://msdn.microsoft.com/en-us/library/ms180175.aspx> for more information.

#### *To create a SQL Login User:*

1. On the SQL Server computer, start SQL Server Management Studio.
2. From the navigation tree in the left pane, select Security > Logins under the SQL instance.
3. Right-click Logins and select New Login from the popup menu to display the New Login dialog box.
4. On the General page, enter a name for the new login, select SQL Server Authentication, enter a password, and clear the Enforce password policy check box.

5. On the Server Roles page, select dbcreator from the list of server roles, and then click OK. The new login user is added to the list in the right pane.

**NOTE:** If upgrading from SQL Server 2000 to SQL Server 2005 in existing QM system, select the db\_datareader and db\_datawriter server roles.

## Configure SQL Server 2005 for QM

After it is installed, the following must be configured so that SQL Server 2005 works with QM:

- Add Windows Firewall exclusions
- Allow remote connections
- Configure SQL Server Browser

### Add Windows Firewall Exclusions

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

#### *To add Windows Firewall exclusions by application:*

1. On the server hosting SQL Server, click Start > Settings > Control Panel > Windows Firewall.

The Windows Firewall application starts.

2. On the Exceptions tab, click Add Program.

The Add a Program dialog box appears, listing all applications loaded on the server.

3. Click Browse and navigate to the SQL Server engine at

C:\Program Files\Microsoft SQL Server\MSQL.1\Binn\sqlservr.exe

**NOTE:** Depending on the number of instances, "MSQL.1" might not be the correct instance.

4. Click OK.
5. In the Windows Firewall window, verify that sqlservr.exe is in the list of Programs and Services and the check box is enabled.

All ports that SQL Server 2005 opens are now accessible.

## Allow Remote Connections

Remote connections are disabled by default. Only connections from the same server are allowed. QM requires remote connections for the following components:

- QM Administrator
- QM Site Configuration Setup
- Reporting
- QM Monitoring and Notification Service

### *To allow remote connections:*

1. Click Start > Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server 2005 Surface Area Configuration.
  2. Under Configure Surface Area for localhost, click Service Area Configuration for Services and Connections.
  3. Select the View by Instance tab, and then expand the tree for the instance configured for QM. Click Remote Connections.
  4. From the options on the resulting window, select:
    - Local and remote connections
    - Using TCP/IP onlyAll other options should be clear.
  5. Click OK.
- Remote connections are now accepted.

## Configure the SQL Server Browser

A new SQL Server component, SQL Server Browser, allows a client to search for named instances. By default, this component is turned off and the service startup type is set to Manual.

If the customer uses a named instance (instead of the default instance), QM requires that this service be running. This step is required only if using a named instance.

### *To configure the SQL Server Browser:*

1. On the server hosting SQL Server, click Start > Settings > Control Panel > Administrative Tools > Services.  
The Windows Services utility starts.
2. In the list of services, locate SQL Server Browser.
3. Right-click the name and choose Properties.

4. In the Properties dialog box, change the startup type from Manual to Automatic.
5. Click Start to start the service, and then click OK.

SQL Server Browser service will now start automatically.

## **Install Windows SNMP Services**

If you intend to use SNMP (Simple Network Management Protocol) to send error messages from the QM services to specified IP addresses, you must install Windows SNMP on the QM Base Services server.

The use of SNMP for notification is configured in QM Configuration Setup or in QM Administrator Site Configuration, in the Monitoring and Notification window.

SNMP allows you to monitor and manage a network from a single workstation or several workstations, called SNMP managers. SNMP is actually a family of specifications that provide a means for collecting network management data from the devices residing in a network. It also provides a method for those devices to report any problems they are experiencing to the management station.

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

### ***To install Windows SNMP:***

1. On the QM Base Services server, select Start > Control Panel and launch the Add or Remove Programs utility.
2. On the left of the Add or Remove Programs window, click Add/Remove Windows Components.
3. From the list of components, select Management and Monitoring Tools, and then click Details.
4. From the list of available components, choose Simple Network Management Protocol and then click OK.
5. You will be prompted for your Windows 2003 CD. Follow the instructions in the installation wizard to install SNMP.

## Installing QM Services

Install the QM services according to the supported system configuration illustrated in [Figure 1 on page 12](#).

QM Configuration Setup runs automatically after you have installed a service or group of services.

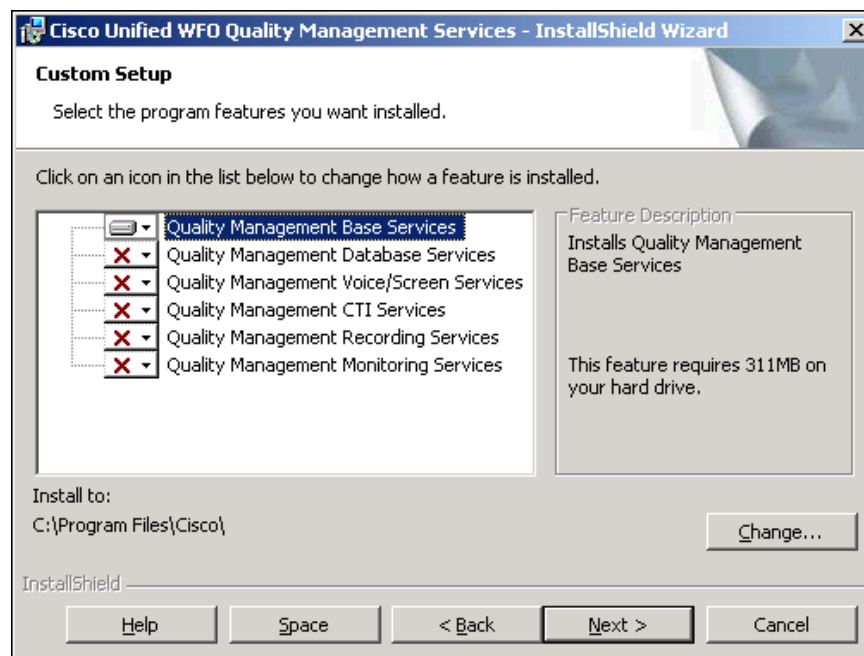
**IMPORTANT!** Any time QM Configuration Setup starts after an installation or an upgrade, it must be run to completion in order for the system to function.

**NOTE:** If you are installing a system that includes screen recording (Advanced bundle), you must configure Proxy Gateway after you have installed the QM services and run QM Configuration Setup. See ["Configuring Proxy Gateway" on page 64](#) for more information.

### To install a QM service or service group:

1. Load the installation CD in the server computer, and then navigate to the CD in My Computer or Windows Explorer.
2. Double-click the file setup.exe to start the installation wizard. The Custom Setup dialog box is displayed ([Figure 4](#)).

Figure 4. Custom Setup window



3. All selected services shown in the dialog will be installed to the server.  
You can change the location where the services will be installed by clicking Change and entering a new path.

4. Click Next, and then click Install.

The services are installed, and QM Configuration Setup starts.

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

5. Complete the QM Configuration Setup windows. See ["QM Configuration Setup" on page 30](#) for more information.
6. Click Finish to complete the installation.

## QM Configuration Setup

---

The QM Configuration Setup tool is used to enter the system configuration information needed for a successful QM installation.

**NOTE:** QM Configuration Setup must be run on the computer hosting the QM Base Services first.

QM Configuration Setup is launched automatically in Initial Mode after you install a QM service. Any time you launch QM Configuration Setup thereafter, it is launched in Update Mode.

QM Configuration Setup does not display the same windows for each service installation, but only those relevant to that service. Depending on where you run QM Configuration Setup, different steps will appear.

The following is a list of all possible steps that can appear when you run QM Configuration Setup.

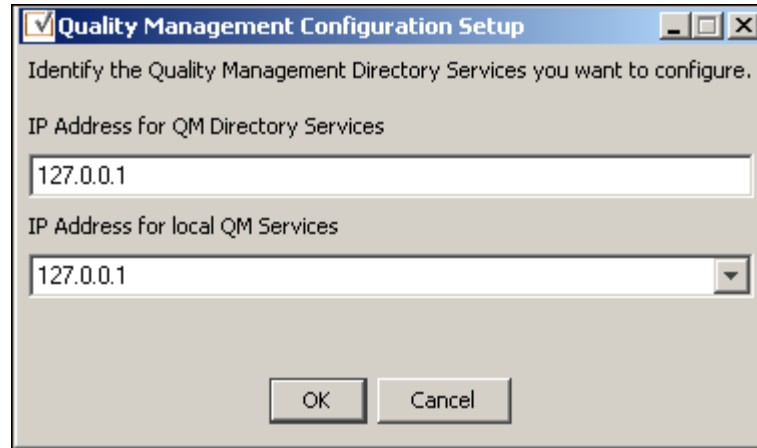
- [Cisco Unified CC Database \(page 33\)](#)
- [Cisco Unified CM \(page 35\)](#)
- [QM Databases \(page 37\)](#)
- [QM CTI Service \(page 39\)](#)
- [Enterprise Settings \(page 40\)](#)
- [Recording File Storage Location \(page 45\)](#)
- [Upload Settings \(page 47\)](#)
- [Monitoring and Notification \(page 49\)](#)
- [Status \(page 62\)](#)

## Entering Configuration Data in Initial Mode

*To enter configuration data in Initial Mode:*

1. Configuration Setup starts automatically and displays the Quality Management Directory Services dialog box (Figure 5).

Figure 5. QM Directory Services dialog box

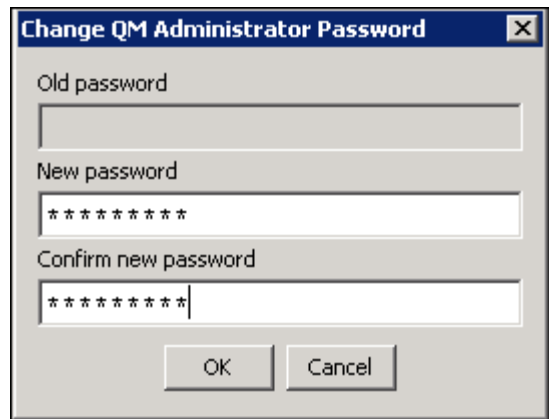


2. Enter the IP address of the computer where the QM Directory Services is located and the IP address of the computer where the QM service you just installed is located, and then click OK.

**NOTE:** If the computer has multiple NIC cards, there will be multiple IPs in the IP Address for local QM Services drop-down list. Choose the IP address used for network traffic.

The Change QM Administrator Password dialog box appears (Figure 6).

Figure 6. Change QM Administrator Password dialog box



3. A password for QM Administrator is required. Enter a password in the New password field, and enter it again in the Confirm new password field. The password must be between 1 and 32 valid Unicode characters long. It is case sensitive.
4. Click OK. The QM Configuration Setup utility appears.
5. Complete the fields in each step. Use the Next button to move forward to the next step.
  - You cannot move forward until all required information is entered.
  - You cannot skip a step.
  - You can go backwards at any time to revisit a previous step.
  - Data you enter in a step is saved when you click Next.

**NOTE:** During Initial Mode, if a step fails, Configuration Setup will stay at the existing step until the step succeeds or is cancelled. The step attempts to run again every time you click Next.

The program carries out any necessary processes and gives you the option of starting the QM services.

6. When you have completed all the configuration steps in the utility, you will see the message, "All QM servers are now installed". Click OK.
7. The Status step is displayed. This step shows the version of all installed QM components.
8. Click Finish to close Configuration Setup.

## QM Configuration Setup Steps

The following are the steps you might see in the QM Configuration Setup utility.

### Cisco Unified CC Database

The Cisco Unified CC Database step (Figure 7) is used to configure the Cisco Unified Contact Center Express database.

The information in this step can be edited only if QM Configuration Setup is running on the QM Base Services server. When viewed on any other machine, it is read-only.

**NOTE:** Do not change the location of the Cisco Unified CC Database after initial setup. If you do, you might be unable to access QM historical data if the structure and contents of the new database is not the same as that of the old database.

Figure 7. Cisco Unified CC Database step

The screenshot shows the 'Cisco Unified CC Database' configuration window. At the top, a note states: 'Note: This information is only editable on the Base Server.' The window is divided into several sections:

- Side A:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field contains '127.00.00.1'.
- Side B:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field is empty.
- SQL Instance Name:** The text field contains 'CRSSQL'.
- Authentication:** Includes radio buttons for 'SQL' (selected) and 'NT'. The 'Login ID' field contains 'sa' and the 'Password' field contains '\*\*\*\*\*'.
- Connection:** Includes radio buttons for 'TCP/IP' (selected) and 'Named Pipe'. The 'Port' field contains '1433'.

At the bottom of the window, there are two buttons: 'Previous' with a left-pointing arrow and 'Next' with a right-pointing arrow.

Table 8. Cisco Unified CC Database step fields

Field	Description
Side A Host Name/IP Address	The host name or IP address of the Cisco Unified CC database.
Side B Host Name/IP Address	The host name or IP address of the redundant Cisco Unified CC database, if one exists.
SQL Instance Name	The SQL Instance name.
SQL or NT	<p>Select the appropriate option to indicate if the database login uses SQL or NT authentication. If you select NT authentication, you must perform the procedure detailed in <a href="#">"Setting Up NT Authentication for the Cisco Unified CC Database"</a> on page 71. Default = NT.</p> <p>This option defines the authentication for QM Directory Services synchronization to the Unified CCX database. The QM Directory Access Synchronization server uses this authentication in order to pull ACD data from Unified CCX. The auto and manual synchronization processes use this account to copy the ACD data from Unified CCX to QM's LDAP database and the QM database.</p>
Login ID	Login ID used to access the Cisco Unified CC database. This user must have write permission to the database.
Password	Password used to access the Cisco Unified CC database.
TCP/IP or Named Pipes	Select the type of connection, TCP/IP or Named Pipes. If you select Named Pipes, you must perform the procedure detailed in <a href="#">"Setting Up Named Pipes for the Cisco Unified CC Database"</a> on page 74.
Port	If you select TCP/IP as the type of connection, enter the port number used to connect to the database. Default = 1433.

### Cisco Unified CM

The Cisco Unified CM step (Figure 8) is used to configure the Cisco Unified CM cluster in your system, including information about the SOAP AXL user and Unified CM (JTAPI) user used by the QM CTI service to log in to the Unified CM.

Figure 8. Cisco Unified CM step

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

You can choose any Unified CM to be your primary and backup. It is recommended that you do not use the Unified CM publisher as the primary CTI Manager.

Each Unified CM in the cluster must be entered in QM Configuration Setup so that QM Recording can find the location of the QM CTI service. QM stores an association between the QM CTI service and the Unified CMs in the cluster. If a Unified CM is not in the list, QM Recording will not know where to register for events.

Table 9. Cisco Unified CM step fields

Field	Description
<b>SOAP AXL Access</b>	
Username	The AXL (Administrative XML Layer) authentication username for this cluster. This is configured when the Unified CM is set up.
Password	The AXL authentication password. This is configured when the Unified CM is set up.
<b>JTAPI User</b>	
Username	The JTAPI user name. This is the application user with which all phone devices are associated in Unified CM. This must be between 1 and 32 alphanumeric characters.
Password	The JTAPI user's password. This must be between 1 and 32 alphanumeric characters.
<b>Cisco Unified Communications Manager Cluster</b>	
Find Subscribers	Click this button to use the AXL user to look up subscribers based on the publisher entered. This is a good way to validate the AXL user and to populate the list of subscribers, if any are found.
Publisher and Subscribers Host Name/IP Address	The host name or IP address of the publisher and subscribers (if any) Cisco Unified CM. You can enter 1 publisher Unified CM, and up to 8 subscriber Unified CMs.
Primary CTI Manager	Select this option if the Unified CM is the primary CTI Manager. There can be only 1 primary CTI Manager. Once entered, a primary CTI Manager can be reassigned, but not deleted.
Backup CTI Manager	Select this option if the Unified CM is the backup CTI Manager. There can be 1 or no backup CTI Manager.
None	Select this option if there is no backup CTI Manager. Default setting = selected.

### QM Databases

The QM Databases window (Figure 9) is used to configure the defined SQL database in which QM information is stored.

Figure 9. QM Databases step

Table 10. QM Database step fields

Field	Description
Host Name/IP Address	The host name or IP address of the QM SQL database server.
SQL Instance Name	The instance name of the QM SQL database server. Leave blank if you want to use the default instance.

Table 10. QM Database step fields — *Continued*

Field	Description
Max Connections	<p>Sets the total number of SQL Server connections that are allocated to QM.</p> <ul style="list-style-type: none"><li>• If the SQL Server is co-resident with the QM services (the CPU-based license model), select the Unlimited check box. This allows as many connections as needed in the connection pools for DB Proxy and reporting.</li><li>• If the SQL Server is offboard (the Client Access License-based model), or if you want to limit the number of connections QM can use with a CPU-based license model, enter the number of connections desired. The range of connections is from 5 to 1000, with a default of Unlimited. Of the connections specified, ~75% are allocated to DB Proxy, ~25% for reporting, and 1 is unallocated for administrative purposes.</li></ul>
Username	The name used to access the QM database (see <a href="#">"Prerequisites" on page 24</a> ).
Password	The password used to access the QM database (see <a href="#">"Prerequisites" on page 24</a> ).

### QM CTI Service

The QM CTI Service step is used to configure the location of the QM CTI service.

Figure 10. QM CTI Service step

Table 11. QM CTI Service step fields

Field	Description
Cluster	(Read only) The publisher IP address of the Cisco Unified Communications Manager cluster to which the CTI service will connect for call events.
Host Name/IP Address	The host name or IP address of the QM CTI service.

## Enterprise Settings

The Enterprise Settings step (Figure 11) enables you to:

- Enable automated software updates for client computers
- Configure Active Directory domains (in an Active Directory system only)
- Configure session timeouts for QM Desktop and QM Administrator
- Enable/disable non-English locales (in a system with non-English versions of QM installed)
- View license information

Before this step appears you will be prompted to define if you use Active Directory or QM Authentication. Which option you select determines if the Active Directory section appears in the Enterprise Settings step.

Figure 11. Enterprise Settings step

**Enterprise Settings**

Software Updates

Enable automatic updates for all QM clients.

Session Timeout Options

Desktop (min)   Unlimited

Administrator (min)   Unlimited

License

Licensed Users **10**

Bundle **Advanced**

Active Directory

Domain	Host/IP Address	Display Name

Add Remove Edit

Locale

English  
English  
French  
German

Previous Next

**NOTE:** The Active Directory section appears in the Enterprise Settings window only if your system is configured to use Microsoft Active Directory. The Locale section appears only if your system has non-English versions of QM installed.

### Software Updates

When you enable automated updates for all QM clients, every time a client application is started, it checks the QM services to determine if a newer version is available. If there is a newer version, it is automatically installed on the client desktop.

### Session Timeout Options

You can configure QM Administrator and/or QM Desktop to do one of the following:

- Close all open popup windows and log out 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 for QM Desktop and QM Administrator, enter the desired number of minutes of inactivity before timeout occurs (from 1 to 1440 minutes) in the minutes field.

**NOTE:** QM Reports uses the same timeout period you configure for QM Desktop.

### Active Directory

The Active Directory section appears only if your system uses Active Directory. Use it to configure Active Directory domains.

- The QM server must be on the same domain or on a trusted domain to the domain that contains the end users who will log in to the QM Desktop
- There must be at least one domain configured
- Each domain must have at least one user path configured

the connection information you enter in the Domain Information dialog box is checked using the entered credentials, and the user paths are validated when you click OK in the Domain Information dialog box.

**To add an Active Directory domain:**

1. Click Add. The Domain Information window appears (Figure 12).

**Figure 12.** Domain Information window

The screenshot shows the 'Domain Information' dialog box with the following fields and values:

- Active Directory Connection:**
  - Base DN: DC=rndcc2,DC=acmi,DC=com
  - Domain Name: rndcc2
  - Host Name: rndcc2.acmi.com (Selected: Host Name)
  - Port: 389
- Active Directory User Credential With Read Access:**
  - Display Name: administrator
  - User Password: \*\*\*\*\*
  - User Search Base: cn=Users
- User Records (OUs):**
  - Path: ou=Users,ou=Minneapolis,ou=Minnesota,ou=US
  - Path: ou=Users,ou=StPaul,ou=Minnesota,ou=US

Buttons at the bottom: Add, Remove, Edit, OK, Cancel.

2. Complete the window as follows, and then click OK. The connection information is checked using the credentials you enter, and the user paths are validated when you click OK.

Table 12. Domain Information window fields

Field	Description
<b>Active Directory Connection</b>	
Base DN	The location in the directory server tree under which all active directory users are located. 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 <i>DC=domain</i> statements to the beginning of the Base DN field.
Domain Name	Defaults to the first part of the string entered in the Base DN field. In most cases this is the domain name, but in some cases the default must be edited.
Host Name/IP Address	The host name or IP address of the Active Directory server.
Port	The port used to access the Active Directory server. The field is autofilled with the default port 389.
<b>Active Directory User Credential with Read Access</b>	
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 LDAP directory under which the user resides. Maximum characters allowed = 1000.

**Table 12. Domain Information window fields – *Continued***

Field	Description
User Records (OUs)	<p>One or more paths to user records (OUs). Click <b>Add</b> to add at least one path, or <b>Remove</b> to remove an existing path. Maximum characters allowed = 1000.</p> <p>LDAP paths must be specified from the most specific to the least specific (from left to right in the path statement). For example, if the AD tree is:</p> <pre>ou=US   ou=Minnesota     ou=Minneapolis       ou=Users</pre> <p>Then the user record is written as follows:</p> <pre>ou=Users,ou=Minneapolis,ou=Minnesota,ou=US</pre>

**To edit or remove an Active Directory domain:**

1. Select the Active directory domain you want to edit or delete from the list in the Path pane.
2. Do one of the following:
  - To edit the selected domain, click Edit, make the desired changes, and then click OK.
  - To delete the selected domain, click Remove.

**Licenses**

The License section displays the number of licensed users and the bundle you have purchased.

Your license can be updated through Unified CCX Licensing.

**Locale**

If non-English versions of QM are installed in your system, use the Locale section to enable the language used in your contact center.

**To enable a locale:**

- Select the desired language from the Locale drop-down box. You can enable only one locale per system.

## Recording File Storage Location

Use the Recording File Storage Location step (Figure 13) to change the location where recordings (screen or voice, depending on which server you are running the Configuration Setup utility) are stored on the server.

Figure 13. Recording Location window

- **Voice Recordings:** You can change the storage location to any local or external folder. It is not necessary that they be stored on the machine hosting the Voice Services.
- **Screen Recordings:** (Advanced bundle only) You can change the storage location to any local or external folder. It is not necessary that they be stored on the machine hosting the Screen Services. If the Screen Services and Voice Services are on the same server, you can elect to use the same path as is used for the voice recordings.

**NOTE:** The File Transfer Servlet that is part of the Voice and Screen services must run as a user with access to whatever location you choose for recordings. To change the recording location:

1. Select if you want to store recordings in a local or external storage location, and then enter the desired location in the Host Name/IP Address and Storage Location fields.
2. If you selected an external location, enter the username and password required to access that location. If the user is a domain user, enter the name with the format <domain>\<username>.

This user meet these requirements:

- The user must be known to the local server (be a trusted domain user)
- If the user is a domain user, the domain specified has to be trusted by the local server. This means the QM Recording Server being configured has to be on a domain that is (or is trusted by) the domain entered.
- The user must be able to log on as a service
- The user must have read/write access to both the external drive location entered AND the location where QM is installed on the local server.

**NOTE:** If you change the storage location from local to external storage, you must first uninstall the Proxy Gateway Service on the server that hosts the QM Voice and Screen services (in Control Panel's Add or Remove Programs, remove Proxy Gateway). When you run the Set Recording Home Directory tool, the Proxy Gateway Service is reinstalled automatically.

3. Click OK.

### Upload Settings

The Upload Settings step (Figure 14) is used to schedule uploading of peak and off-peak recordings from the agent desktops to the Voice and Screen servers, as well as recording metadata to the QM database.

Figure 14. Upload Settings step

Table 13. Upload Settings step fields

Field	Description
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.

Table 13. Upload Settings step fields — *Continued*

Field	Description
Max Peak Hour Uploads	The maximum number of recordings that can be simultaneously uploaded during peak hours. Must be a value from 1 to 100. This limit is set to conserve bandwidth on the network. As one upload is completed, 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 be simultaneously uploaded 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. As one upload is completed, another takes its place, but there can be no more than the configured number uploading at any one time. Default = 100.
Database Cleanup Time	The time when the DBCleanup utility runs. This utility deletes expired recordings from the database. Must be between 00:00 and 23:59 in 1-minute increments. It is recommended that you choose a time when no uploads are occurring to reduce the load on the system. Default = 00:05.
<b>Recording Servers (appears after the Screen and Voice services are installed)</b>	
Screen Server	(Read-only) The IP address of the machine that hosts the Screen services and screen recordings, and the path where screen recordings are stored. If the Basic bundle is installed, this does not appear.
Voice Server	(Read-only) The IP address of the machine that hosts the Voice services and the voice recordings, and the path where voice recordings are stored.

## Monitoring and Notification

The Monitoring and Notifications step (Figure 15) is used to enable the monitoring and notification feature, and to configure the following:

- Method used to notify administrators/supervisors of a system problem
- Email address of the person(s) receiving notification, if email is set up to be the means of notification
- Trap destinations receiving notification, if SNMP is set up to be the means of notification
- If and how often a renotification of the problem should be sent out
- Types of problems that will trigger notification.

Figure 15. Monitoring and Notifications step

**Monitoring and Notification**

Use Monitoring/Notification Service

Notification

Use Event Viewer Notification

Use SNMP Notification SNMP Configuration \*

Use Email Notification SMTP Configuration \*

Email Addresses

Add Remove Edit

Properties

Polling Period (in min) 10

Renotification Period

Never

Every 3 Polling Periods

Every Polling Period

Available Problems

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

Enabled Problems

ID	Description	Setup
QM2003	No phone could be detected on a PC.	
QM1006	A Quality Management service is using more memory than it should. It might fail soon.	

\* SMTP and SNMP may only be configured from the QM Base Server

Previous Next

Table 14. Monitoring and Notification step fields

Field	Description
Use Monitoring/Notification Service	Enable this check box to use the Monitoring and Notification (Mana) Service. If enabled, at least one notification method (event viewer, SNMP, or email) must be enabled as well.
<b>Properties</b>	
Polling Period	Sets the interval at which the Mana service checks for the selected notification triggers. Default = 10 min. Minimum = 0 min., Maximum = 1440 min. (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.
<b>Notification</b>	
Use Event Viewer Notification	Enable this check box to use the Event Viewer for displaying notification messages.
Use SNMP Notification	Enable this check box to use SNMP for sending out notification messages. Note that the Windows SNMP Services must be installed in order to be able to use SNMP notification. See <a href="#">"Install Windows SNMP Services" on page 27</a> for more information.
SNMP Configuration	Click this button to configure the SNMP connection (enabled only on the Base Services server).
Use Email Notification	Enable this check box to use email for sending out notification messages.
SMTP Configuration	Click this button to configure the SMTP email connection (enabled only on the Base Services server). See <a href="#">"Configuring Email Addresses for Notification" on page 52</a> for more information.
Email Addresses	The list of email addresses to which notification is sent. Maximum = 5 email addresses.
Add	Click this button to add an email address.
Remove	Click this button to remove the selected email address.
Edit	Click this button to edit the selected email address.
<b>Renotification Period</b>	

Table 14. Monitoring and Notification step fields — *Continued*

Field	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 and enter how frequently you want renotification to occur after the initial notification. 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.
Available Problems	The list of problems that can trigger notification if enabled by using the arrow keys to move them to the Enabled Problems pane. By default only one problem, QM3002, is not enabled and in this list.
Enabled Problems	The list of enabled problems. By default, all problems except for QM3002 are enabled. If QM3002 is enabled, a Setup button appears in the Setup column. Click this button to configure the Call Detail Record (CDR) task. See <a href="#">"Configuring Notification Problems" on page 55</a> for more information.

#### Configuring SNMP for Notification

you can use SNMP notification if the Microsoft Simple Network Management Protocol (SNMP) service is installed on the QM Base services server.

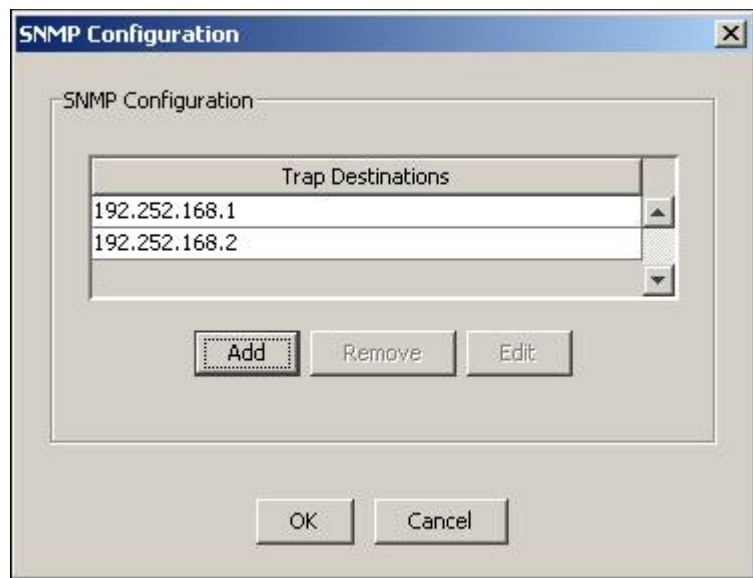
**NOTE:** You will not be able to configure SNMP unless the Windows SNMP service is installed on the QM Base services server. You will not be able to select SNMP notification on a non-Base services server unless SNMP is configured on the QM Base services server.

If you select the Use SNMP Notification check box, MANA notification messages are sent from the QM services server to specified IP addresses. Use the Configure SNMP button to manage the list of destination IP addresses.

For more information on using this tool, see Microsoft SNMP documentation. For information on installing the Windows SNMP services, see ["Install Windows SNMP Services" on page 27](#).

**To configure the SNMP settings:**

1. Click SNMP Configuration The SNMP Configuration dialog box appears.

**Figure 16. SNMP Configuration dialog box**

2. Do one of the following:
  - Click Add to add a new trap destination.
  - Select a listed trap destination and then click Edit to change the IP address.
  - Select a listed trap destination and then click Remove to delete the IP address.
3. When you have finished, click OK to save your changes.
4. 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.

**Configuring Email Addresses for Notification**

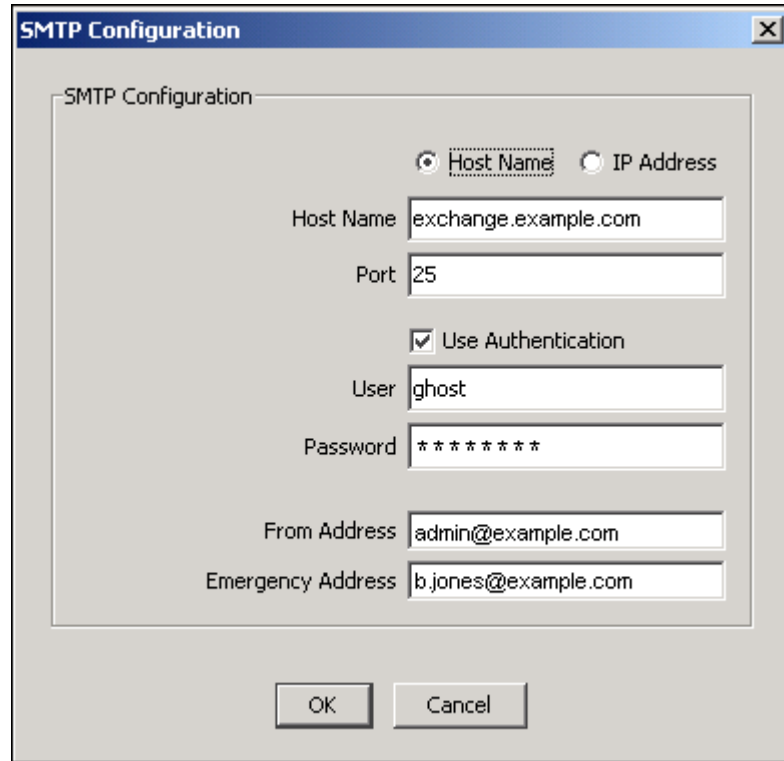
Notifications can be sent to either the Event Viewer or in emails to specified recipients. To use email notification, enable the Use Email Notification check box and then configure up to 5 email addresses.

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

To configure the SMTP settings for email:

1. Click SMTP Configuration. The SMTP Configuration dialog box appears (Figure 17).

Figure 17. SMTP Configuration dialog box



2. Complete the fields as follows, and then click OK.

Table 15. SMTP Dialog Box Fields

Field	Description
Host Name/IP Address	Choose Host Name or IP Address, and then enter the host name or IP address of the SMTP server.
Port	The port used by the Mana service to communicate with the SMTP server.
Use Authentication	Enable this check box if authentication is needed to access the SMTP server.
User	The user name needed to access the SMTP server.

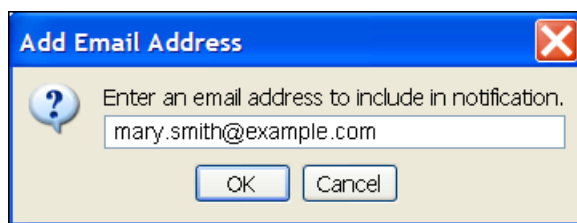
**Table 15. SMTP Dialog Box Fields — Continued**

Field	Description
Password	The password needed to access the SMTP server.
From Address	The email address from which all notification emails will come.
Emergency Address	<p>The email address to which notification is sent if LDAP 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 LDAP, and thus will not be functional in the event that LDAP is unavailable when the Mana service first starts.</p> <p>If the Mana service has already obtained a valid configuration from LDAP, and then LDAP 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 LDAP is down will go to the configured email address, not to the emergency address.</p>

**To add a notification email address:**

1. In the Monitoring and Notification window's Notification section, click Add. The Add Email Address dialog box appears (Figure 18).

**Figure 18. Add Email Address dialog box**



2. Type the email address to which you want notifications sent, and then click OK. The email address is added to the list.

**To edit or remove a notification email address:**

1. In the list of email addresses, select the email address you want to edit or remove.

2. Do one of the following:
  - To edit the address, click Edit, make the necessary changes in the Edit Email Address dialog box, and then click OK.
  - To remove the address from the list, click Remove.

**Configuring Notification Problems**

Currently, only one notification problem trigger requires configuration: Problem ID QM3002. This problem compares data in the Cisco Unified Communications Manager (Unified CM) Call Detail Record database (for Unified CM version 4.x) or CAR Report (for Unified CM versions 5.x, 6.x, and 7.x) with the QM database. Specifically, it compares the call records in the Unified CM with the call records in QM. If there is a discrepancy, notification is sent.

By default, Problem ID QM3002 is disabled. The problem does not have to be configured unless you enable that problem ID in the list of notification triggers.

Prerequisites to configuring the CDR task notification problem are:

- CDR is correctly configured in the Unified CM Administration web application.
  - Unified CM 4.x: See Service > Service Parameters. By default, the CDR database is not set up for SQL authentication. SQL authentication must be set up and a read-only user configured for QM.
  - Unified 5.x, 6.x, and 7.x: See Serviceability > Tools. In these versions, there is no CDR database. Instead, the CAR reports (CDR export) are used. Set up CAR so that it updates its information as frequently as possible, at a minimum, at less than 30-minute intervals. Create a CAR user and enter that user in the QM CDR Configuration dialog.
- Archiving in QM is enabled.

**To configure the CDR task notification problem:**

1. Click Setup. The Configuration dialog box appears (Figure 19).
2. Complete the fields as follows, and then click OK.

**Table 16. Notification Trigger Configuration fields**

Field	Description
<b>CDR Configuration</b>	
Add, Remove, Edit buttons	Use these buttons to add, edit, and remove information about the Cisco Unified CM from which the Call Detail Record or CAR report information will be obtained.
<b>Ignored Extensions</b>	

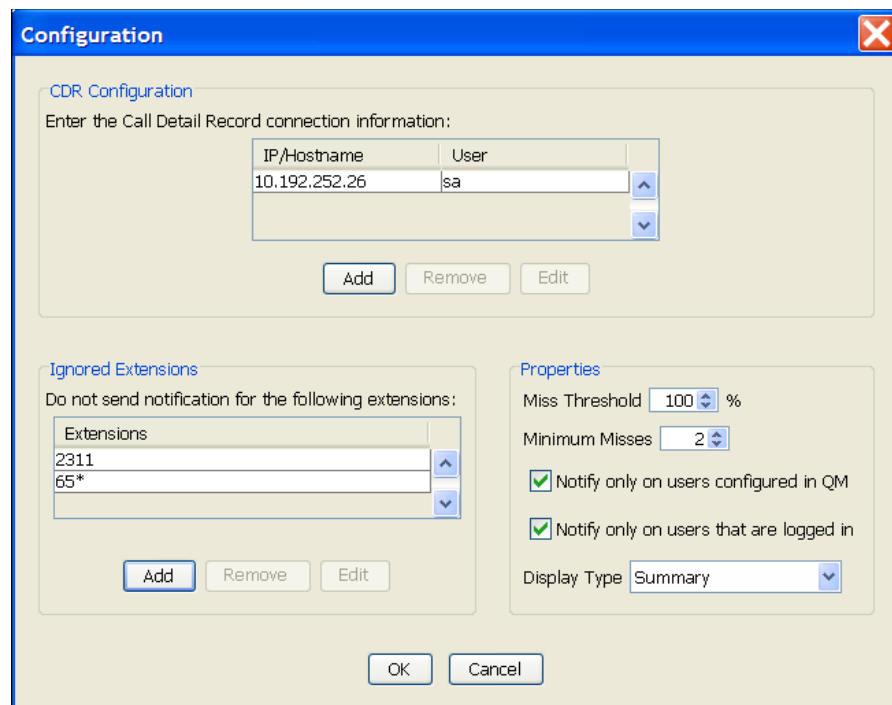
Table 16. Notification Trigger Configuration fields — *Continued*

Field	Description
Add, Remove, Edit buttons	Use these buttons to add, edit, or remove extensions that are to be excluded from notification triggered by Problem ID QM3004. The extensions can be exact strings, or use the wild cards * and ?. Extensions in this list will still be recorded.
<b>Properties</b>	
Miss Threshold	The percentage of calls for each agent that must be missed before notification is sent. Default = 100%. Percentage is calculated by: $\text{missed} / (\text{found} + \text{missed})$ Both the Miss Threshold and the Minimum Misses threshold must be met before notification is sent.
Minimum Misses	The lowest number of calls that must be missed before notification is sent. Default = 2. Both the Miss Threshold and the Minimum Misses threshold must be met before notification is sent.
Notify on users configured in QM	Enable this check box to trigger notification on all users who are configured and licensed in QM. Default = Enabled. If not enabled, the system will notify on all extensions that receive calls according to CDR, if they are configured or not.
Notify on users who are logged in	Enable this check box to trigger notification on only those QM users who are logged in at the time of the call. Default = Enabled. If not enabled, the system will notify on any extension that has been associated with an agent, whether or not that agent is currently logged in to QM.

Table 16. Notification Trigger Configuration fields — *Continued*

Field	Description
Display Type	<p>Select the format in which you want to display the report. Default = Summary Only.</p> <ul style="list-style-type: none"> <li>• Summary Only</li> <li>• Detail (Tab Delimited)</li> <li>• Detail (Plain Text)</li> </ul> <p>See "<a href="#">CDR Information Formats</a>" on page 60 for more information.</p>

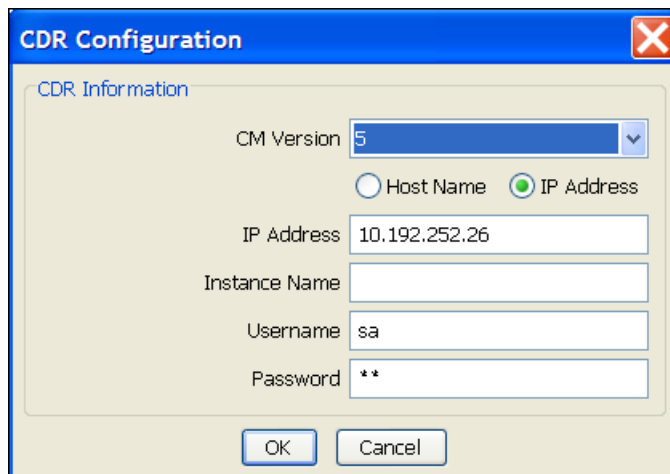
Figure 19. Configuration dialog box



**To add Call Detail Record connection information:**

1. In the CDR Configuration section, click Add. The CDR Information dialog box appears (Figure 20).

**Figure 20. CDR Information dialog box**



2. Complete the fields as follows, and then click OK.

**Table 17. CDR Configuration dialog box fields.**

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.
Instance Name	Enabled only if using Unified CM 4.x. The instance name of the Unified CM database. Usually the default instance of the CDR database is used, so this field can be blank.
User Name	(Unified CM 4.x) The name of the user with rights to access the Unified CM database. (Unified CM 5.x, 6.x, 7.x) The name of the user with rights to access the CAR reports.
Password	(Unified CM 4.x) The password of the user with rights to access the Unified CM database. (Unified CM 5.x, 6.x, 7.x) Te password of the user with rights to access the CAR reports.

The CDR connection information you entered appears in the list.

**To edit or remove Call Detail Record connection information:**

1. In the list of CDR connections, select the connection you want to edit or remove.
2. Do one of the following:
  - To edit the connection, click Edit, make the necessary changes in the CDR Configuration dialog box, and then click OK.
  - To remove the connection from the list, click Remove.

**Examples of Notification Trigger Configuration**

The following illustrate what happens when Notification Trigger Configuration is set up as described.

**Setup 1:** Miss Threshold: 50%; Minimum Misses: 5; Notify on users configured in QM: Enabled; Notify on users logged in: Enabled.

**Agents:** Agent A has 8 matched calls and 2 missed calls. Agent A is properly configured and was logged in for the whole time.

Agent B has 6 matched calls, but 2 were made before he was logged in. Agent B is configured properly.

Agent C has 2 matched calls and 8 missed calls. Agent C is properly configured and was logged in the whole time.

**Effect:** Agent A: The missed percentage is  $2/(8 + 2) = 20\%$ . No notification would be made because neither the Miss Threshold or the Minimum Misses threshold were met.

Agent B: No notification would be made because the Minimum Misses (5) was not met.

Agent C: The missed percentage is  $8/(2 + 8) = 80\%$ . Notification is made because the Miss Threshold and the Minimum Misses threshold were met.

**Setup 2:** Miss Threshold: 100%; Minimum Misses: 1; Notify on users configured in QM: Enabled; Notify on users logged in: Disabled.

**Agent:** Agent A is configured in QM but does not have the QM Recording client installed, or the phone is not daisy-chained properly.

**Effect:** Notification will be made on Agent A's extension, with the agent listed as 'Unknown' because there is no cross-reference between the agent and extension until the QM Recording client is configured.

**NOTE:** Matching the CDR or CAR Report with QM is not 100% accurate. CDR data can be out of sync with QM, or certain call scenarios might yield false positives. It should not be used for compliance.

When a notification is received, look at the DNs/Agents that show missed calls. A large number of agents with missed calls might indicate a QM service failure. The possible services with issues are:

- QM CTI service
- QM Upload Controller
- QM DBProxy service (on the QM Database server)

A 100% miss percentage for a single agent might indicate a failure in the QM Recording client. If notifications are occurring frequently with less than 100% missed for a small number of agents, the thresholds might need to be adjusted to minimize unnecessary notifications. Even a high threshold (100%) will notify on moderate and major outages.

#### CDR Information Formats

You can specify in which format you want to display the CDR information in the Notification Trigger Configuration dialog box (see ["Configuring Notification Problems" on page 55](#)). Examples of the available formats are listed here.

**NOTE:** In these reports, call durations are expressed in milliseconds.

**NOTE:** If the agent is listed as “Unknown” it means the agent hasn't successfully logged in recent history on a PC that has the QM Recording client. It is probable that these agents are not configured correctly. Notifications for unknown agents are filtered out if the “Configured in QM” check box is enabled.

#### Summary Only

Status Report

Start Time: 01/11/2008 15:25:53

End Time: 01/11/2008 16:25:53

Extensions with Missed Calls:

Ext	Agent	Found	Missed	% Missed
1545	JonesM	0	8	100%
2201	SmithB	0	15	100%

#### Detailed (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 03:29:36	13000
16778560	JonesM	1545	2671	1545	01/11/2008 03:29:52	14000
16778561	JonesM	1545	2671	1545	01/11/2008 03:30:09	7000
16778562	JonesM	1545	2671	1545	01/11/2008 03:30:20	8000
16778594	JonesM	1545	2671	1545	01/11/2008 03:36:01	12000
16778596	JonesM	1545	2671	1545	01/11/2008 03:36:18	11000

**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):

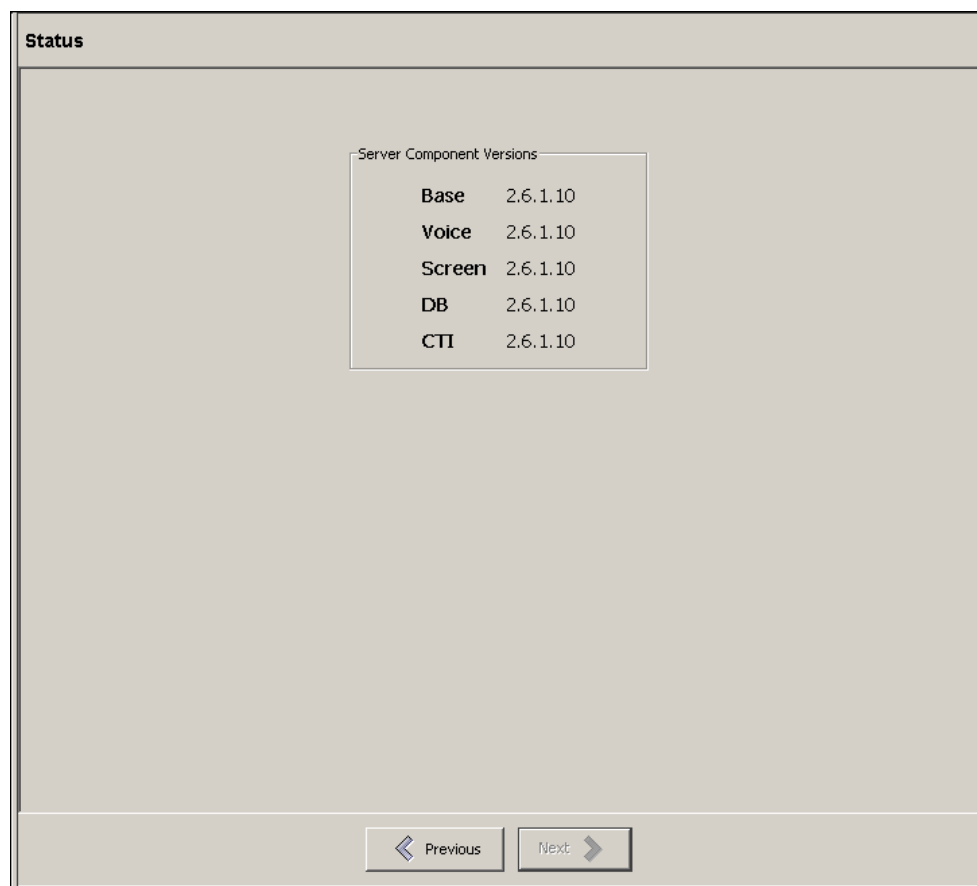
Call ID = 16778554  
 Agent = JonesM  
 Ext = 1545  
 ANI = 2671  
 DNIS = 1545  
 Start = 01/11/2008 03:29:36  
 End = 01/11/2008 03:29:49  
 Duration= 13 sec

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

## Status

The status step (Figure 21) displays which version of each QM component is installed.

Figure 21. Status step



## Entering Configuration Data in Update Mode

There are two ways to change configuration setup data after it is initially entered.

- Change the information through the Site Configuration node in QM Administrator.
- Start QM Configuration Setup from the executable PostInstall.exe, located on each server in C:\Program Files\Cisco\WFO\_QM\bin.

When QM Configuration Setup is started, it runs in Update Mode.

***To change configuration setup data in Update Mode:***

1. Start QM Configuration Setup.
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 but haven't saved yet, and reverts the window back to the last saved version.
3. When you are done making your changes, choose File > Exit or click Close.  
QM Configuration Setup closes.
4. Stop and restart the modified service and all desktops for the change to go into effect.

## Configuring Proxy Gateway

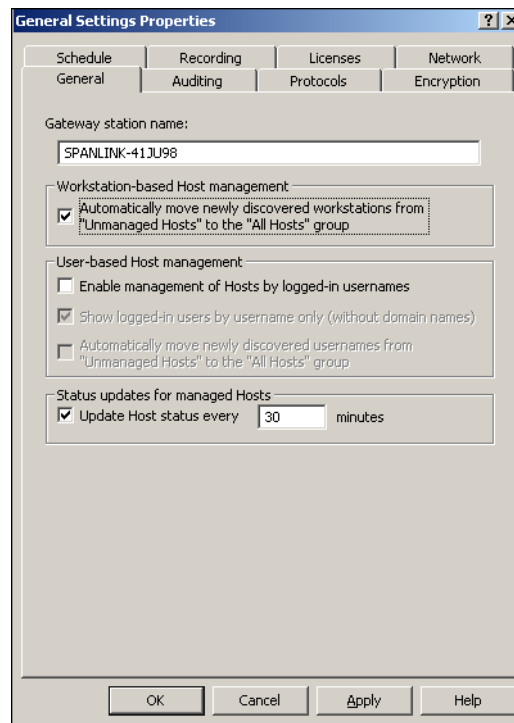
This section applies only to systems that include screen recording (Advanced bundle).

After you have installed the QM services and have successfully run QM Configuration Setup, you must manually configure the Proxy Gateway permissions for administrators on the server that hosts the QM Network Recording service and the server that hosts the Screen service.

**To configure Proxy Gateway permissions for administrators:**

1. On the server that hosts the QM Network Recording service and the server that hosts the QM Screen service, launch Proxy Gateway Administrator (Start > Programs > Proxy Networks > Proxy Gateway Administrator).
2. From the navigation tree in the left pane, choose Local Gateway > Gateway Server Settings > General Settings.
3. Right-click the General Settings node and select Properties from the popup menu. The General Properties Settings dialog box appears (Figure 22)

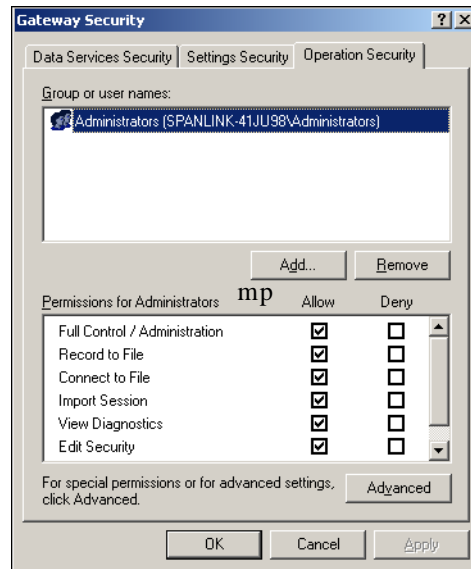
**Figure 22. General Settings Properties dialog box**



4. Select the Automatically move newly discovered workstations from “Unmanaged Hosts” to the “All Hosts” group check box and then click OK.

5. In the navigation tree, select the Gateway Security Node, and from the right pane, click the link “Click here to change Operation Security.” The Gateway Security dialog box appears (Figure 23).

**Figure 23. Gateway Security dialog box**



6. On the Operation Security tab, enable permissions for administrators as follows:
  - On the server hosting the QM Network Recording service, select the Allow check box for Record to File.
  - On the server hosting the QM Screen service, select the Allow check box for Connect to File.
7. Click OK.

## QM Configuration Setup Tools

There are a number of tools available to run when you update site information with QM Configuration Setup. These tools are available through the Tools menu (Figure 24). These tools normally run during the initial installation of QM.

Tools are enabled as appropriate for the server on which you are running Configuration Setup, as described in Table 18.

Figure 24. QM Configuration Setup tools

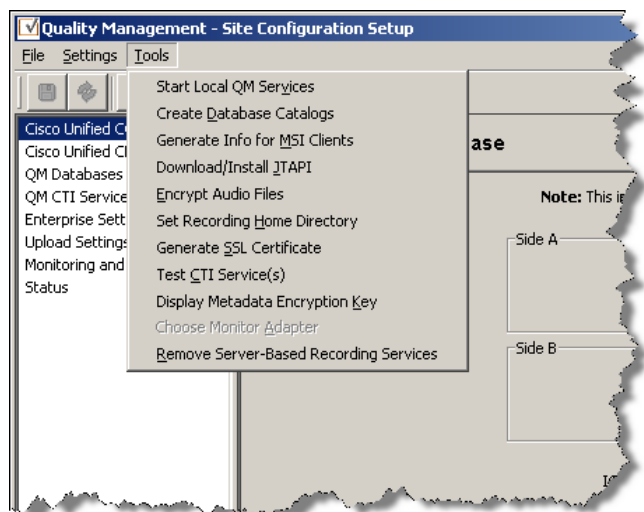


Table 18. Tool availability based on the server on which QM Configuration Setup is run

Tool	Server						
	Base	Database	Voice	Screen	CTI	Monitor	Recording
Start Local QM Services	x	x	x	x	x	x	x
Create Database Catalogs	x	x					
Generate Info for MSI Clients	x						
Download/Install JTAPI					x		
Encrypt Audio Files			x				
Set Recording Home Directory			x	x			
Generate SSL Certificate	x		x	x			

Table 18. Tool availability based on the server on which QM Configuration Setup is run

Tool	Server						
	Base	Database	Voice	Screen	CTI	Monitor	Recording
Test CTI Service(s)	x	x	x	x	x	x	x
Display Metadata Encryption Key	x	x	x	x	x	x	x
Choose Monitor Adaptor						x	
Remove Server-Based Recording Service	x	x	x	x	x	x	x

### Start Local QM Services

This tool offers a convenient way to start all the QM services that are on the local computer.

### Create Database Catalogs

This tool creates a new QM 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 to recreate your QM database if you have no backup and your database was corrupted and you deleted it. The fresh database will be populated when the Unified CCX and LDAP databases are synced with it.

### Generate Info for MSI Clients

This tool updates the information required by the MSI client installation programs to successfully install QM Desktop, QM Recording, and QM Administrator.

### Download/Install JTAPI

This tool is used when a Unified CM is upgraded. It downloads and installs JTAPI.

### Encrypt Audio Files

Audio files were not encrypted in QM 2.1. They are encrypted in QM 2.6. When upgrading from version 2.1 to 2.6, some audio files might be left in the staging folders on the client machines during the upgrade process and get uploaded after the upgrade without being encrypted. This tool enables you to encrypt any audio files that are not already encrypted. The only time this tool should be run is after all client desktops are upgraded to QM 2.6. After that time, no audio files will be unencrypted.

## Set Recording Home Directory

This tool displays the Recording Location window (see ["Recording File Storage Location" on page 45](#)) so you can change the location where recordings are stored. This step must be run when upgrading from the Basic to the Advanced bundle.

**NOTE:** If you change the storage location from local to external storage, you must first uninstall the Proxy Gateway Service on the server that hosts the QM Voice and Screen services (in Control Panel's Add or Remove Programs, remove Proxy Gateway). When you run the Set Recording Home Directory tool, the Proxy Gateway Service is reinstalled automatically.

## Generate SSL Certificate

This tool generates a security certificate for the File Transfer Servlet (FTS) and QM Desktop-generated reports. Use the tool if the certificate becomes corrupt or if the IP address of the server changes (the user will see a Security Alert dialog box whenever the FTS or Reports runs). This tool is available only when Configuration Setup is run on the Base Service server (for reporting) and the Voice Services and Screen Services server (for FTS).

When you run the tool, you will 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 Service(s)

This tool verifies that the local QM CTI Service has the correct JTAPI and will accept connections. The tool makes a request to each QM CTI Service and, if all succeed, returns a success message. If any fail, it reports the failure and lists which succeed.

## Display Metadata Encryption Key

This tool shows the information required to access user-defined metadata directly from the QM database. The dialog box shows the customer-specific key used for AES encryption.

## Choose Monitor Adaptor

This tool is a dialog that asks for the IP address of the NIC card that will be used for the QM Monitor service and server-based monitoring. This might be different from the network IP address entered during QM Configuration Setup.

The monitor adapter dialog pops up automatically during QM Configuration Setup if multiple NIC cards are on the box and the box hosts the QM Monitor service. You should choose the IP address of the NIC card that is plugged in to the SPAN port on the switch.

### **Remove Server-Based Recording Service**

This tool is used to finalize the removal of QM Recording Service servers and QM Monitoring Service servers by removing them from LDAP. Do this only after you have uninstalled the services from the server.

## Upgrading from Previous Versions

---

QM 2.4 can be upgraded to QM 2.6 with over-the-top installation. There is no need for manual backing up and restoring of data.

QM 2.3 must be backed up and uninstalled before installing QM 2.6. The data you backed up from 2.3 can then be restored to 2.6.

**NOTE:** Any installed Service Release software associated with the previous version will be automatically uninstalled during an over-the-top upgrade.

Consult the release notes for the most up-to-date details of the upgrade procedure.

## Setting Up NT Authentication for the Cisco Unified CC Database

---

If you select NT Authentication on the Cisco Unified CC Database window in QM Configuration Setup ([page 33](#)), you must perform the following procedure to support NT authentication for the Cisco Unified CC database.

These steps must be done after you install the QM Base Services and before you start administering any users with QM Administrator.

To set up NT authentication for the Cisco Unified CC database, you perform the following three procedures.

1. Set up NT users who will be used to connect to the database.
2. Configure the QM Sync Service to run as the authenticating user.
3. Allow the user access to the Cisco Unified CC database.
4. Verify the connection.

### Set Up NT Users

Follow these steps to set up NT users who will be used to connect to the database. A user must be known on both the Unified CCX server and the QM server, and the Unified CCX server cannot be on a domain.

On the Unified CCX server:

1. Add a user.
2. Add this user to the CiscoCRSUsers and Administrator groups.

On the QM server:

1. Add a user with the same username and password as the user created on the Unified CCX server.
2. Add this user to the Administrator group
3. Set the user to have permissions to log on as a service.

**To add a user:**

1. Right-click My Computer and select Manage.
2. Under Local Users and Groups, right-click Users and select New User.
3. Enter a username and password, clear the User must change password at next logon check box, select the Password never expires check box, and then click Create.

The user is now added to the list of users.

**To add a user to a group:**

1. Under Local Users and Groups, right-click the user, choose Properties, and select the Member of tab.
2. Click Add, and then click Advanced.
3. Click Find Now, and from the resulting list select the groups you want the user to belong to.
4. Click OK to close the Select Groups dialog box, and OK again to close the User Properties dialog box.

**To give a user permissions to log on as a service:**

1. In Control Panel, select Administrative Tools > Local Security Policy.
2. In the left pane, select Local Policy > User Rights Assignment, and in the right pane, double-click Log on as a service.
3. In the resulting dialog box, click Add User or Group, and then enter the username or click Find Now to select the username from a list, and then click OK.

## Configure the QM Sync Service

Follow these steps to configure the QM Sync Service to run as the authenticating user.

1. On the computer hosting the QM Base services, open the Services utility in Control Panel (under Administrative Tools).
2. Right-click the Quality Management Sync Service and choose **Properties** from the popup menu.
3. On the Log On tab, choose This Account and enter the username and password of the Windows user whose credentials you want to use for authentication.

**NOTE:** the Windows user must have write access to the ...\\Calabrio\\WFO\_QM\\log folder so logs can be written.

**NOTE:** If you are using Named Pipes as the connection protocol, the username and password you enter here must be the same one you used when setting up Named Pipes. See ["Setting Up Named Pipes for the Cisco Unified CC Database" on page 74.](#)

## Verify the Connection

Follow these steps to verify the connection between QM and the Unified CC database.

1. Start QM Administrator.

2. Click Personnel > User Administration, and select the Unlinked Users tab (for systems that use Active Directory) or the Unconfigured Users tab (for systems that do not use Active Directory). If there are users listed there, the synchronization worked.

**To allow the user access to the Cisco Unified CC database:**

1. On the computer that hosts the Cisco ICM (for Unified CCE systems) or Cisco CRS (for Unified CCX systems), open the MS SQL Server Enterprise Manager and navigate to the Security node under the Cisco Unified CC database instance (which might be the default instance).

The Logins node displays a list of Windows and SQL users who can access the databases in this instance. Check to see if the Windows user you configured in Procedure 1 is in the list. If not, you must create a new login. If the user already exists, skip to Step 3.

2. To create a new login:
  - a. Right-click Logins and choose New Login from the popup menu.
  - b. On the General tab, enter the user name from Procedure 1 in the Name field. In the Authentication section, select Windows Authentication, select or enter the user's Windows domain in the Domain field, and select Grant access.
  - c. Click OK to add the new login to the list.
3. Right-click the login and choose Properties from the popup menu.
4. On the Database Access tab, select <dbname>\_sideA in the list of databases. In the Database Roles pane, select db\_datareader.
5. Repeat Step 4 for <dbname>\_sideB.
6. Click OK.

## Setting Up Named Pipes for the Cisco Unified CC Database

---

If you select Named Pipes on the Cisco Unified CC Database window in QM Configuration Setup ([page 33](#)), you must perform the following procedure to support Named Pipes for the Cisco Unified CC database.

**NOTE:** QM supports only the default SQL Server pipe name. The default pipe name is \\<hostname>\pipe\sql\query.

These steps must be done after you install the QM Base Services and before you start administering any users with QM Administrator.

To set up Named Pipes on the Cisco Unified CC database, you must:

1. Configure the QM Sync Service to run as the authenticating user.
2. Verify that Named Pipes is a valid protocol with the default pipe name.
3. Verify the connection.

### **1. To configure the QM Sync Service to run as the authenticating user:**

1. On the computer hosting the QM Base services, open the Services utility in Control Panel (under Administrative Tools).
2. Right-click the Cisco Quality Management Sync Service and choose Properties from the popup menu.
3. On the Log On tab, choose This Account and enter the username and password of the Windows user whose credentials you want to use for authentication.

**NOTE:** If you are using NT authentication, the username and password you enter here must be the same one you used when setting up authentication. See "[Setting Up NT Authentication for the Cisco Unified CC Database](#)" on [page 71](#).

### **2. To verify that Named Pipes is a valid protocol with the default pipe name:**

1. On the computer that hosts the Cisco ICM, open the MS SQL Server Enterprise Manager and navigate to the SQL Server instance for the Cisco Unified CC database.
2. Right-click the SQL Server instance and choose Properties from the popup menu to display the SQL Server Properties (Configure) dialog box.
3. On the General tab, click Network Configuration to display the SQL Server Network Utility dialog box.

4. Verify that Named Pipes is in the list of enabled protocols.
5. Select Named Pipes and then click Properties to display the Named Pipes dialog box.
6. Verify that the Default Pipe field displays `\\.pipe\sql\query` or `\\<hostname>\sql\query`.

**3. To verify the connection:**

1. On the QM Base Services server, start the Cisco Quality Management Sync Service.
2. Open the DirAccessSyncServer.log file located in the C:\Program Files\QM\log folder.
3. Verify that the follow message is in the log:  
FCSS0021 SetServerStatus Change server to active.  
and that there are no major or minor error messages present.

## Installing QM Desktop Applications

---

### Overview

QM desktop applications are installed from web pages that are created when the Base Services are installed. These web pages are:

- **Administrator.htm.** This page contains links to the install files for all three desktop applications—QM Administrator, QM Desktop, and QM Recording.
- **Desktop.htm.** This page contains a link to the QM Desktop install files.
- **Recording.htm.** This page contains a link to the QM Recording install files.

**NOTE:** Install the QM desktop applications after all the QM services have been installed.

### Enabling the Elevated Privileges Policy for Windows Installer Installations

To allow users with limited privileges to be able to install a desktop application on their computer (for example, an evaluator installing his or her own instance of QM Desktop) 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 enable the Windows elevated privileges policy:*

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the appropriate organizational unit (OU) and from select Properties from the popup menu.
3. On the Group Policy tab, select the Group Policy Object (GPO) and then click Edit.
4. Expand Computer Configuration > Administrative Templates > Windows Components > Windows Installer.
5. Double-click Always install with elevated privileges.
6. Set to Enabled, and then click OK.
7. Expand User Configuration > Administrative Templates > Windows Components > Windows Installer.

8. Double-click Always install with elevated privileges.
9. Set to Enabled, and then click OK.

**NOTE:** You must enable this GPO under both the User Configuration and Computer Configuration sections for it to take effect.

## Installation Procedure

Follow these steps to install the QM desktop applications.

### *To install QM desktop applications:*

1. From the computer where you want to install the desktop application, start Internet Explorer.
2. Enter the appropriate installation web page address in the Address field:
  - <http://<base services IP address>:8088/TUP/QM/Administrator.htm>
  - <http://<base services IP address>:8088/TUP/QM/Desktop.htm>
  - <http://<base services IP address>:8088/TUP/QM/Recording.htm>The installation web page appears.

3. Follow the instructions on the web page to install the desktop application.

**NOTE:** When installing QM Desktop, an icon for JMStudio is added to the user's desktop and the JMStudio application is left open on the user's computer. The application should be closed and the icon can be deleted if desired.

## **Using Automated Package Distribution Tools**

QM's MSI-based desktop application installations can be deployed ("pushed") via automated package distribution tools that make use of the Microsoft Windows Installer service.

### **Requirements**

QM support for automated package distribution depends on compliance with the requirements listed below.

#### **Execution**

Installations must be executed on the target machine. Deployment methods that capture a snapshot of an installation and redistribute that image are not supported.

#### **Per-Machine vs. Per-User Installation**

Installations must be deployed on a per-machine basis. Per-user installations are not supported.

#### **Privileges**

QM installations require either administrative or elevated privileges.

By default, Windows Installer installations run in the context of the logged-on user.

If the installation is run in the context of an administrative account, there is no need to enable policies to grant elevated privileges.

If the installation is run in the context of an account with reduced privileges, then it must be deployed with elevated privileges. The target machine must have the Windows policy "Always Install with Elevated Privileges" enabled for both the User Configuration and the Computer Configuration. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the installation to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

#### **Automated Package Installation vs. Manual Installation**

Automated installations must use the same files and meet the same installation criteria as manually-deployed installations.

QM MSI packages are located in the following location on a successfully-installed production server and are intended for both manual and automated deployment.

<user-defined path>\WFO\_QM\Tomcat\webapps\TUP\QM

You can also generate QM MSI packages using the ConfigureMsi.exe utility and unconfigured installation templates, available on the QM installation CD. See "[Client Installation Packages on the Installation CD](#)" on page 80 for more information.

Alteration of these files or the use of other MSI files included with the product at other locations is not supported.

Installation criteria such as supported operating systems, product deployment configurations, installation order, and server/client version synchronization must be met. Altering the supplied MSI packages to circumvent the installation criteria is not supported.

### Multiple Software Releases

Multiple software releases must not be combined into a single deployment package. Each QM software release is intended for distribution in its entirety as a distinct deployment. Combining multiple releases (for example, a software package's base release and a subsequent service release) into a single deployment package is not supported.

### Reboots

Any reboots associated with QM installations are required. If the installation's default reboot behavior is suppressed, the target machine must be rebooted before running the installed applications to ensure expected functionality.

Delaying a reboot is not known to be an issue at this time, as long as a reboot occurs before launching the installed applications. If it is determined in the future that delaying a reboot via command line suppression affects expected behavior, then that delayed reboot will not be supported.

## Best Practices

Best practices recommendations are listed below.

### Windows Installer Logging

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

```
/l*v <logfile path and name>
```

**NOTE:** The logfile path and name must be a location to which the installation's user context has permission to write.

This ensures that any loggable issues are captured efficiently.

## Deployment

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

## Installation and Uninstallation Deployment Packages

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

## Recommended Deployment Preparation Model

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment. This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in ["Requirements" on page 78](#).
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.

## Client Installation Packages on the Installation CD

The QM installation CD contains unconfigured installation templates that, with the use of a configuration tool (ConfigureMsi.exe), can be configured so that client applications are available prior to the installation of the QM services.

The unconfigured installation templates are located in the following file structure on the installation CD:

```
Clients
  Admin
  Playback
  Recording
  SR
```

### *To configure client installation files with the ConfigureMsi tool:*

1. Copy the Clients folder and all its contents from the QM installation CD to a PC that does not have the QM Base services installed on it.
1. On the desktop, open a command window and navigate to the Clients folder.

2. Type ConfigureMsi and press Enter. The configuration tool starts and displays a list of available languages. Choose the number of the language you want the client applications to use and press Enter.
3. Type the IP address of LDAP Host 1 and press Enter. The utility creates installation files for all QM client applications.

**NOTE:** The base release and service releases of the same version of software can be combined into a single folder structure, since the configuration tool will detect and configure both types of install packages.



---

## Removing QM

# 3

---

### Removing QM

---

Uninstall QM in the following order:

1. QM service releases, if any
1. QM Recording
2. QM client applications
3. QM services

Recordings are not removed from client or server computers when QM is removed. They are maintained in the folder located at:

Server: C:\Program Files\Common Files\QM\Recordings  
Clients: C:\Program Files\Common Files\SQM\Recordings

Note that this is the default location and that a custom location might have been set up for your system.

**NOTE:** A user must be logged in as an Administrator in order to remove any QM applications.

**To remove a QM application:**

1. Open the Windows Control Panel.
2. Double-click Add/Remove Programs.
3. From the list, select the application you wish to remove and click Remove.  
The application is removed.

**NOTE:** If you have multiple QM client applications installed on one computer, and wish to uninstall one application and leave the rest, you must uninstall all of the applications, reboot your computer, and then reinstall the desired set of applications. The

applications share certain third party files, and uninstalling one application may remove files needed by the remaining applications.

**NOTE:** If you intend to reinstall QM after completely removing an older version (a clean install), verify that the recording storage folder structures are removed before installing the new version.

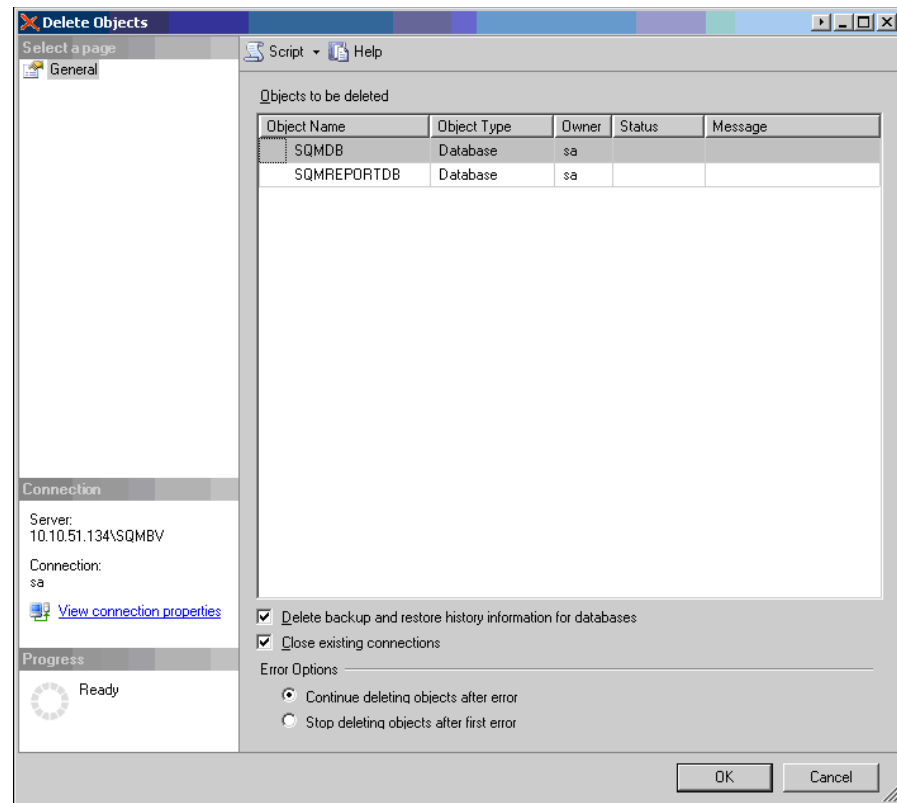
Using the Windows Control Panel to remove services will not remove the QM databases (SQMDB, SQMREPORTDB, and Hibernate). If you are intending to reinstall or upgrade QM, and you want to retain historical data, the QM databases must not be removed. However, if you want to remove QM completely, follow this procedure to remove the databases.

***To remove the QM databases:***

1. On the server that hosts the QM databases, 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 (

**Figure 25.** Delete Object window



4. Select the Close existing connections check box and then click OK.
5. Repeat steps 2-4 for the SQMREPORTDB and Hibernate databases.



---

# Index

---

<b>A</b>	prerequisites 24 procedure 28
Active Directory domain adding 42	<b>L</b>
Automated package distribution tools 78	LDAP 9
<b>C</b>	<b>M</b>
CallManager Clusters window 35	Microsoft SQL Server 2005 installation 24
CDR information formats 60	Monitoring and Notification window 49
<b>D</b>	<b>N</b>
DBCleaner service 9	Named pipes 74
DBProxy service 9	Notification trigger reports 60
DBSync service 9	Notification triggers 55
<b>E</b>	NT authentication 71
Elevated privileges 76	<b>P</b>
Enterprise Settings window adding an Active Directory domain 42	Pushing desktop installations 78
<b>F</b>	<b>Q</b>
File Transfer Servlet (FTS) 9	QM Administrator about 9
<b>I</b>	QM components 9
Installation order 23	CTI service 9
Installing Microsoft SQL Server 2005 24	DBCleaner service 9
Installing QM desktop applications 76	DBProxy service 9
enabling elevated privileges 76	DBSync service 9
procedure 77	File Transfer Servlet (FTS) 9
using automated package distribution tools 78	LDAP 9
Installing QM services	QM Administrator 9
	QM Desktop 9
	QM Recording 9

---

QM Configuration Setup 30  
    CallManager Clusters window 35  
    entering data in Update Mode 62  
    tools 66  
QM CTI service 9  
QM Desktop  
    about 9  
QM installation order 7  
QM Recording  
    about 9

---

## R

Removing QM applications and services 83  
Reports, notification trigger 60

## S

Setting up named pipes 74  
Setting up NT authentication 71  
Site configuration  
    Monitoring and Notification window 49