



Cisco Unified Workforce Optimization

Quality Management Installation Guide 2.4
October 2007

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0704R)

Quality Management Installation Guide

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

Overview 7

- Introduction 7
- QM 2.4 Components 8
 - Client Applications 8
 - QM Administrator 8
 - QM Desktop 8
 - QM Recording 8
 - Services 8
 - CTI Service 8
 - DBCleaner Service 8
 - DBProxy Service 8
 - DBSync Service 9
 - File Transfer Servlet (FTS) 9
 - LDAP 9
 - LDAP Monitor Service 9
 - Sync Service 9
 - Tomcat Webserver 9
 - Upload Controller Service 9
- System Configuration 10
- System Requirements 12
 - System Environment 12
 - Data Configuration Environment 12
 - Operating Environment 12
 - Server Capacity Guidelines 13
 - Sizing Guidelines 14
 - Remote Agent Requirements 14
 - Supported IP Phones 14
 - Supported Cisco Unified Outbound Dialer Modes 15
 - Required Third Party Applications 15
- Firewall Requirements 16
- QM Recording Requirements 17
 - Required Phone Device Parameters 17

Contents

Required Codecs	17
Hard Drive Space on Agent Computers	17
QM Recording and Network Interface Cards	18
QM Recording Phone Configurations	19

Installing QM 21

- Introduction 21
- Prerequisites 22
 - Install Microsoft SQL Server 2005 22
 - Configure SQL Server Firewall Port Exceptions 23
- Installing QM Services 25
- QM Configuration Setup 27
 - Entering Configuration Data in Initial Mode 27
 - QM Configuration Setup Windows 29
 - Cisco Unified CC Database 29
 - QM Databases 31
 - Enterprise Settings 33
 - Recording File Storage Location 36
 - Upload Settings 38
 - Cisco Unified CM 40
 - QM JTAPI Installation 41
 - Status 43
 - Entering Configuration Data in Update Mode 43
 - QM Configuration Setup Tools 44
 - Start Local QM Services 44
 - Create Database Catalogs 45
 - Generate Info for MSI Clients 45
 - Download/Install JTAPI 45
 - Encrypt Audio Files 45
 - Set Recording Home Directory 45
 - Generate SSL Certificate 45

Contents

- Upgrading from Previous Versions 46
- Setting Up NT Authentication for the Cisco Unified CC Database 47
 - Set Up NT Users 47
 - Configure the QM Sync Service 48
 - Verify the Connection 48
- Setting Up Named Pipes for the Cisco Unified CC Database 51
- Installing QM Desktop Applications 53
 - Overview 53
 - Enabling the Elevated Privileges Policy for Windows Installer Installations 53
 - Installation Procedure 54
- Using Automated Package Distribution Tools 55
 - Requirements 55
 - Execution 55
 - Per-Machine vs. Per-User Installation 55
 - Privileges 55
 - Automated Package Installation vs. Manual Installation 55
 - Multiple Software Releases 56
 - Reboots 56
 - Best Practices 56
 - Windows Installer Logging 56
 - Deployment 56
 - Installation and Uninstallation Deployment Packages 57
 - Recommended Deployment Preparation Model 57

Removing QM 59

- Removing QM 59

Index 61

Contents

Overview

1

Introduction

Quality Management (QM) 2.4 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

QM 2.4 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.

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.

DBCleaner Service

The DBCleaner 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.

DBProxy Service

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

DBSync Service

The DBSync service synchronizes LDAP with the QM database.

File Transfer Servlet (FTS)

The File Transfer Servlet uses HTTP protocol to upload files from agent desktops to the Voice and Screen servers.

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.

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.

Sync Service

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

Tomcat Webserver

The Tomcat webserver hosts the QM Reports engine, the recording upload engine, and the licensing engine.

Upload Controller Service

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

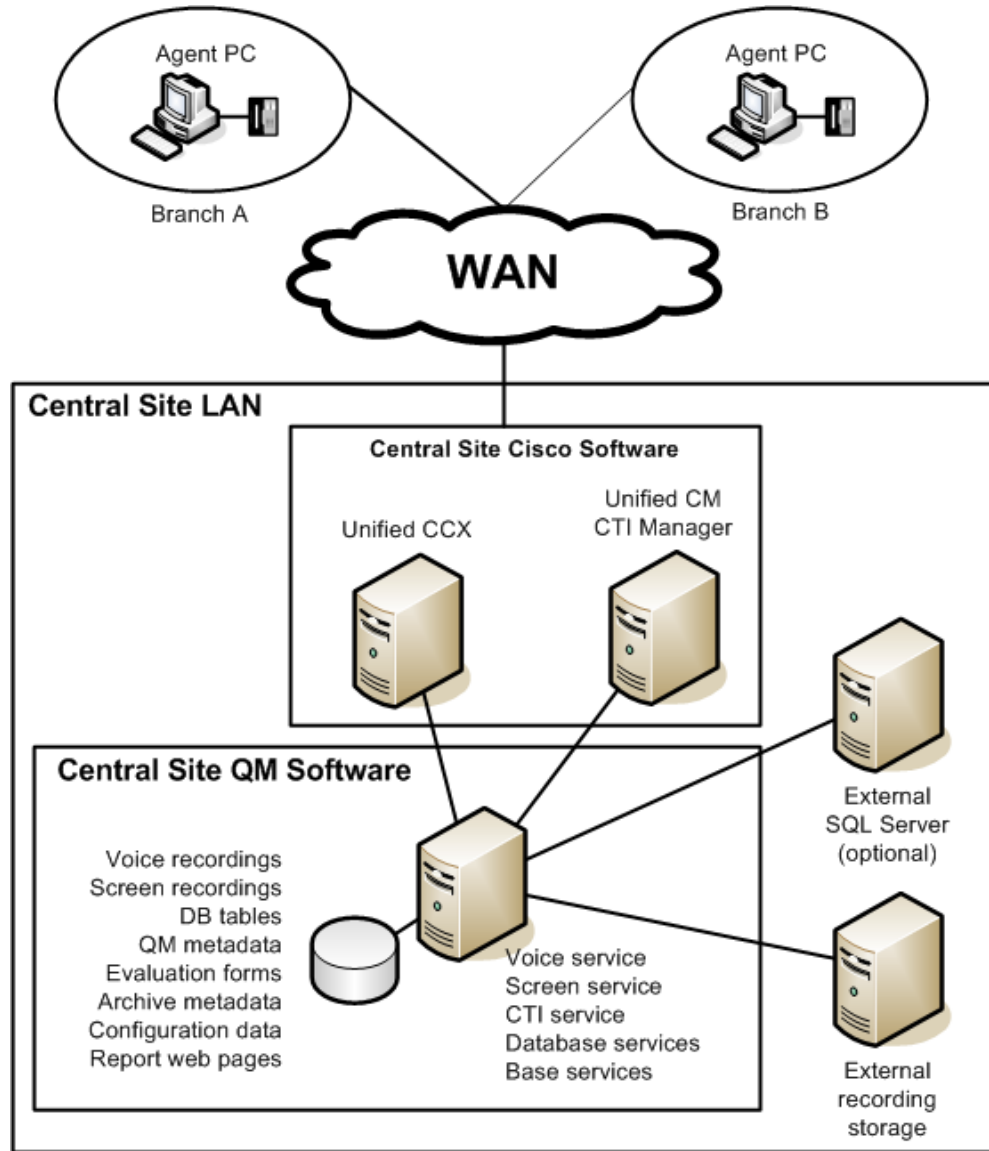
System Configuration

One system configuration is supported. This configuration is able to use an external storage server to store/archive voice and screen recording files (see "[Installing QM Desktop Applications](#)" on page 53). The supported configuration is illustrated in [Figure 1](#).

NOTE: A single deployment supports either the Standard bundle of QM or the Enhanced 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 2.4 is integrated into the following Cisco Unified Contact Center Express (Unified CCX) environment:

Table 1. System environment

ACD	Cisco Unified Communications Manager
Unified CCX 5.0	5.1, 6.0
Unified CCX 6.0	6.0

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 2.4 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 Standard Bundle	QM Recording Enhanced Bundle
Windows 2000 Professional, Service Pack 4 or later	1 GHz processor 256 MB RAM 20 GB disk space 100+ MB NIC*	500 MHz processor 256 MB RAM 100+ MB NIC*	1 GHz processor 512 MB RAM 100+ MB NIC*
Windows XP Professional, Service Pack 2 or later	1 GHz processor 256 MB RAM 20 GB disk space 100+ MB NIC*	500 MHz processor 256 MB RAM ??? disk space 100+ MB NIC*	1 GHz processor 512 MB RAM ??? disk space 100+ MB NIC*

Table 2. Supported desktop component operating systems and hardware – *Continued*

Operating System	Minimum Hardware Requirements		
	QM Administrator QM Desktop	QM Recording Standard Bundle	QM Recording Enhanced Bundle
Windows Vista Business, Enterprise, and Ultimate Editions	1 GHz processor 1 GB RAM 40 GB disk space 100+ MB NIC*	1 GHz processor 1 GB RAM 40 GB disk space 100+ MB NIC*	1.5 GHz processor 1 GB RAM 40 GB disk space 100+ MB NIC* NOTE: QM 2.4 does not support screen recording in a Vista environment. These are preliminary hardware specs pending the availability of screen recording in Vista in the future.

* NICs must support Promiscuous Mode. For a list of supported NICs, see http://www.cisco.com/application/pdf/en/us/guest/products/ps14/c1221/cdcont_0900aecd800e3149.pdf

Table 3. Supported QM central server operating systems and hardware

Operating System	Minimum Hardware Requirements
Windows 2003 Server R2 Standard 5 Client Access Licenses (CAL)	Cisco Media Convergence Server (MCS) platform or exact equivalent. For a list of supported MCS-equivalent platforms see http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html

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

Named Users	Concurrent Agents	Server Hardware
up to 450	up to 150	MCS-7816-H3-CCX1
up to 900	up to 300	MCS-7825-H3-CCX1 MCS-7835-H3-CCX1 MCS-7845-H3-CCX1

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 on-site are supported only if they connect to the network via a Cisco 831 router and use a supported hard phone. Cisco IP Communicator is not supported for remote agents.

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

Cisco IP Phone Model	Protocol
7940	SCCP
7960	SCCP
7970	SCCP/SIP
7911G	SCCP/SIP
7912G-A	SCCP
7941G	SCCP/SIP
7941G-GE	SCCP/SIP
7961G	SCCP/SIP
7961G-GE	SCCP/SIP
7971G	SCCP/SIP
IP Communicator Soft Phone	SCCP

For the most up-to-date list of supported IP phones, see the list of IP phones for desktop/endpoint monitoring in the *Cisco Customer Response Solutions (CRS) Software and Hardware Compatibility Guide*, available online at www.cisco.com.

Supported Cisco Unified Outbound Dialer Modes

QM 2.4 supports the Direct Preview dialing mode.

Required Third Party Applications

QM 2.4 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 Administrator QM Desktop	HTML-based reports
Adobe Acrobat Reader 6.0 or later	QM Administrator QM Desktop	PDF-based reports and QM user documentation. Free download at www.adobe.com
Microsoft SQL Server 2005	QM Database server	Database

Firewall Requirements

For QM to function correctly, the ports in [Table 7](#) must be opened in the Windows firewall before QM is installed. If the Microsoft 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 Microsoft Firewall after QM is installed, these ports must be opened manually. See your firewall documentation for instructions.

Table 7. QM Port Usage

Port	Type	Description
7	TCP	Echo port
1433*	TCP	MSSQL server port (named instance)
1434	UDP	MSSQL server port
2303	UDP	Funk port
8088	TCP	Tomcat port
8448	TCP	File Transfer Servlet (FTS) port
38983	TCP	LDAP port
52102	TCP	CTI port
52103	TCP	DB Proxy port
59100	TCP	Controller port
DirAccessSynSvr.exe	—	Sync service

* If the default instance is used, the TCP port is 1433. If a different instance is used, the port number is randomly assigned. See ["Configure SQL Server Firewall Port Exceptions" on page 23](#) for instructions on determining the randomly-assigned port number.

QM Recording Requirements

Required Phone Device Parameters

For QM 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 and G.729 codecs. 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 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.

QM Recording and Network Interface Cards

QM 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 Recording Phone Configurations

Two phone configurations are supported:

- Hard IP phone and agent computer daisy-chained to the network (see [Figure 2](#)). Multiple daisy-chained phones are not supported.
- Cisco IP Communicator soft phone on the agent's computer, connected to the network (see [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 Recording.

NOTE: Shared lines are not supported.

Figure 2. QM Recording hardware setup (hard IP phone),

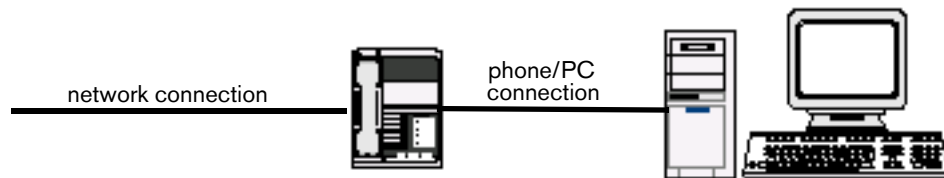
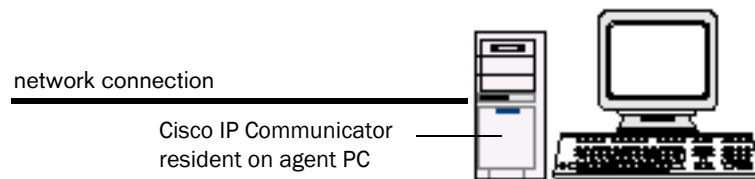


Figure 3. QM Recording hardware setup (Cisco IP Communicator soft phone).



Introduction

QM is installed in this order:

1. Install QM services
2. Run QM Configuration Setup
3. Install QM client applications

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

Prerequisites

Before you install the QM services:

- Install Microsoft SQL Server 2005, either co-resident with the QM Database service or on an off-board server
- Configure the port exceptions in the Windows firewall (if the firewall is turned on) for the Microsoft SQL Server

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 SQL_Latin1_General_Cp1_CI_AS: see [http://msdn2.microsoft.com/en-us/library/aa258233\(SQL.80\).aspx](http://msdn2.microsoft.com/en-us/library/aa258233(SQL.80).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.
6. Click **OK**.

The new login user is added to the list in the right pane.

Configure SQL Server Firewall Port Exceptions

Before QM is installed, you must manually add two ports to the firewall exception list on the QM Database services server. This procedure is necessary only if the Microsoft firewall is turned on. These ports are:

Port	Type	Description
1433	TCP	MSSQL server port (named instance)
1434	UDP	MSSQL server port

The default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances are configured for dynamic ports, which means they select an available port when the SQL Server service is started. When connecting to a named instance through a firewall, configure the Database Engine to listen on port 1433, so that the appropriate port can be opened in the firewall.

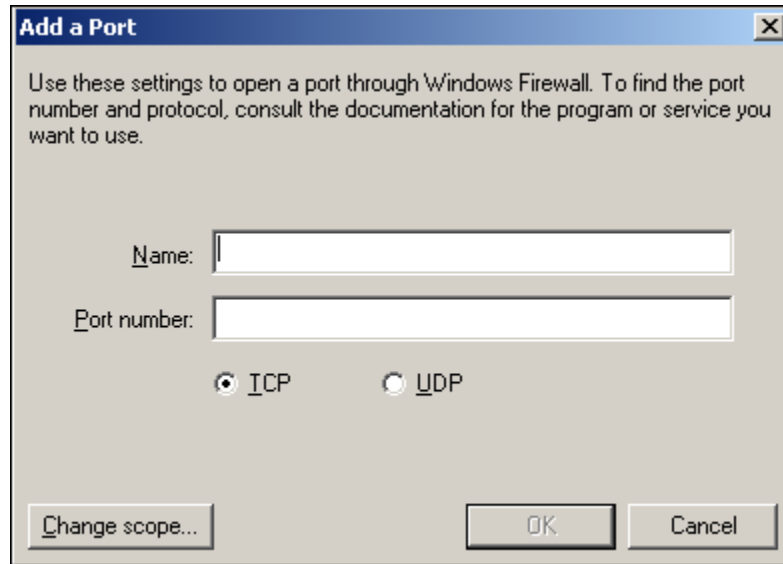
To determine the randomly assigned port number:

1. On the SQL Server computer, start SQL Server Configuration Manager.
2. From the navigation tree in the left pane, expand **SQL Server 2005 Network Configuration > Protocols for <instance name>**, and then in the right pane, double-click **TCP/IP**.
3. In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear, in the format IP1, IP2, and IPAll. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP address on the computer. Determine which IP address you want to configure.
4. If the **TCP Dynamic Ports** field for that IP address contains **0**, indicating the Database Engine is listening on dynamic ports, delete the 0.
5. In the **TCP Port** field, type the port number **1433**, and then click **OK**.
6. In the left pane, click **SQL Server 2005 Services**.
7. In the right pane, right-click **SQL Server (<instance name>)** and from the popup menu, click **Restart**, to stop and restart SQL Server.

To add the ports to the firewall exceptions list:

1. On the SQL Server computer, start the Windows Firewall utility and select the **Exceptions** tab.
2. Click **Add Port** to display the Add a Port dialog box.

Figure 4. Add a Port dialog box.



3. For the MSSQL server port named instance, enter a name describing the port, the port number **1433**, select **TCP** as the connection type, and then click **OK**.
4. Click **Add Port** again, and for the MSSQL server port, enter a name describing the port, the port number **1434**, select **UDP** as the connection type, and then click **OK**.

Installing QM Services

Install the QM services according to the supported system configuration illustrated in [Figure 1 on page 11](#).

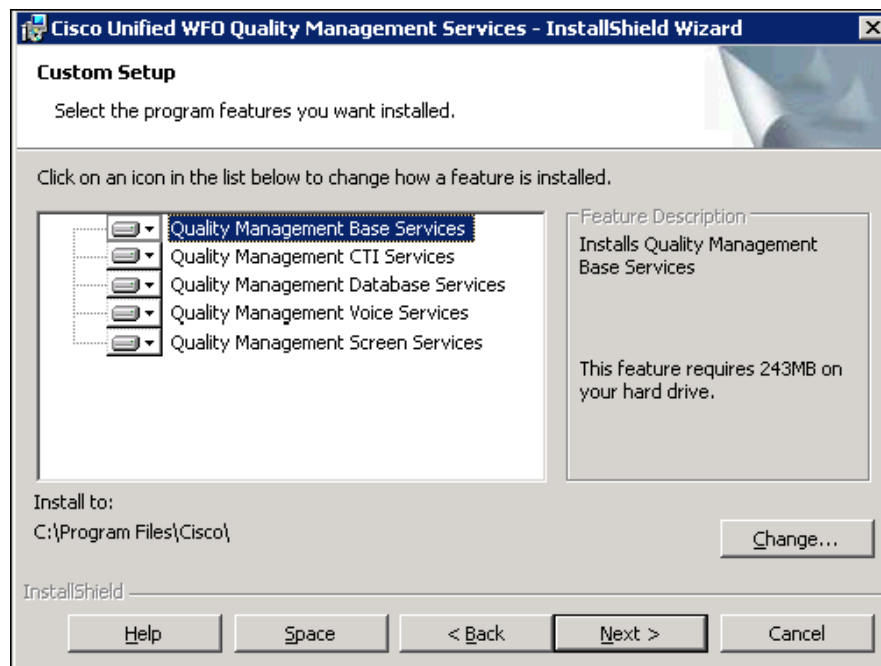
QM Configuration Setup runs automatically after you have installed a service or group of services.

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.

To install a QM service or service group:

1. If present on the server, stop Cisco Security Agent.
2. Load the installation CD in the server computer, and then navigate to the CD in My Computer or Windows Explorer.
3. Double-click the file **setup.exe** to start the installation wizard. The Custom Setup dialog box is displayed (see [Figure 5](#)).

Figure 5. Custom Setup window.



4. All 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.

5. 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.

6. Complete the QM Configuration Setup windows. See "[QM Configuration Setup](#)" on page 27 for more information.
7. Click **Finish** to complete the installation.
8. If present on the server, restart Cisco Security Agent.

QM Configuration Setup

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

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.

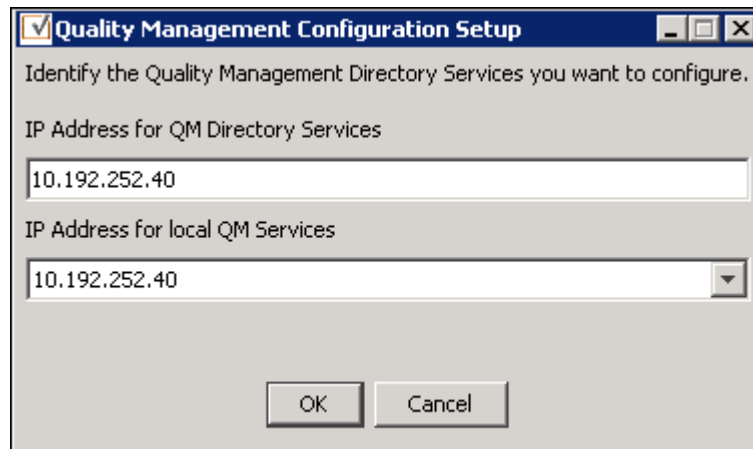
Entering Configuration Data in Initial Mode

After a QM service is installed, QM Configuration Setup starts automatically. It does not display the same windows for each service installation, but only those relevant to that service.

To enter configuration data in Initial Mode:

1. Configuration Setup starts automatically and displays the Quality Management Directory Services dialog box (see [Figure 6](#)).

Figure 6. 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**.

The Change QM Administrator Password dialog box appears (see [Figure 7](#)).

Figure 7. Change QM Administrator Password dialog box.



3. By default, there is no password. Enter your new password in the New password field, enter it again in the Confirm new password field, and then click **OK**.

The password must be between 1 and 32 alphanumeric characters long. It is case sensitive.

The QM Configuration Setup utility appears.

4. Complete the fields in each window. Use the Next button to move forward to the next window.
 - You cannot move forward until all required information is entered.
 - You cannot skip a window.
 - You can go backwards at any time to revisit a previous window.
 - Data you enter in a window is saved when you click Next.

NOTE: During Initial Mode, if a step fails, Configuration Setup will stay at the existing window 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.

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

QM Configuration Setup Windows

The following are the windows you may see in the QM Configuration Setup utility.

Cisco Unified CC Database

The Cisco Unified CC Database window (see [Figure 8](#)) is used to configure the Cisco Unified Contact Center Express database.

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 8. Cisco Unified CC Database window.

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 '192.168.252.66'.
- Side B:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field is empty.
- SQL Instance Name:** The field contains 'CR5SQL'.
- Authentication:** Includes radio buttons for 'SQL' and 'NT' (selected). The 'Login ID' field contains 'Administrator' 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 arrow) and 'Next' (with a right arrow).

Table 8. Cisco Unified CC Database fields

Field	Description
Side A IP Address/ Host Name	The IP address or host name of the Cisco Unified CC database, depending on which radio button is selected.
Side B IP Address/ Host Name	The IP address or host name of the redundant Cisco Unified CC database, if one exists, depending on which radio button is selected.
SQL Instance Name	The SQL instance name. Default = CRSSQL.
SQL or NT	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 "Setting Up NT Authentication for the Cisco Unified CC Database" on page 47 . Default for Unified CCX systems = NT.
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	Enter the type of connection, TCP/IP or Named Pipes. If you select Named Pipes, you must perform the procedure detailed in "Setting Up Named Pipes for the Cisco Unified CC Database" on page 51 .
Port	If you select TCP/IP as the type of connection, enter the port number used to connect to the database. Default = 1433.

QM Databases

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

Figure 9. QM Databases window.

Table 9. QM Database fields

Field	Description
IP Address	The IP address of the machine where the QM SQL database server is hosted. This field appears only if the IP Address option is selected.
Host Name	The host name of the machine where the QM SQL database server is hosted. This field appears only if the Host Name option is selected.
SQL Instance Name	The instance name of the QM SQL database server. Leave blank if you want to use the default instance name.

Table 9. QM Database fields — *Continued*

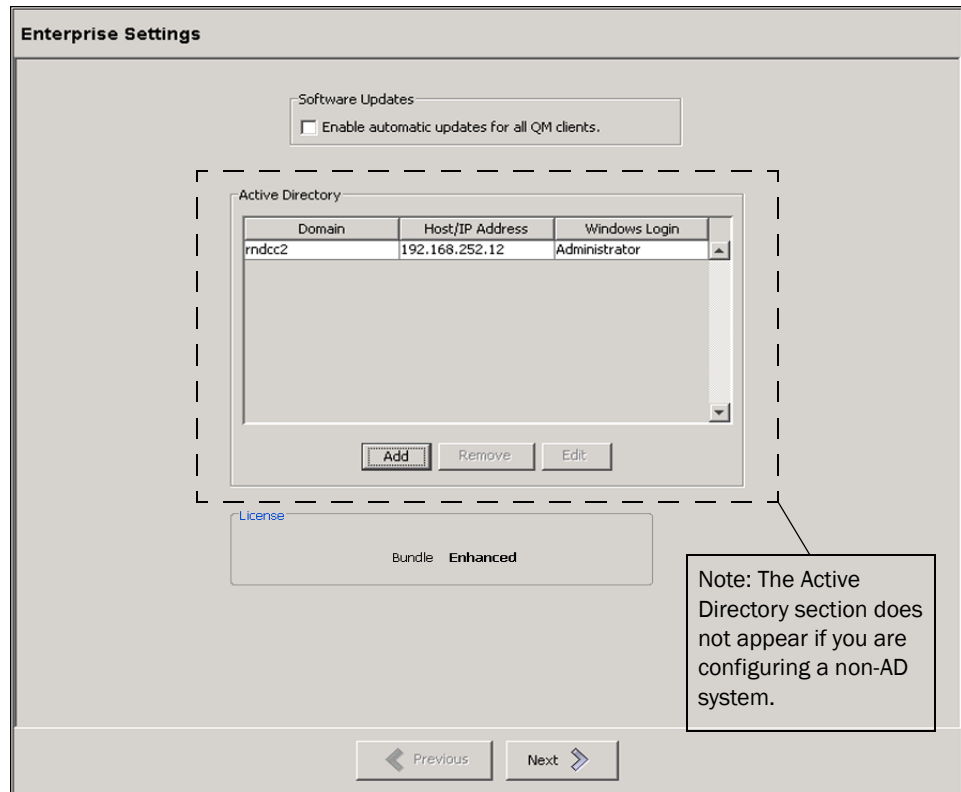
Field	Description
Max Connections	<p>Sets the total number of SQL Server connections that are allocated to QM.</p> <ul style="list-style-type: none">• If the SQL Server is co-resident with the QM services (the CPU-based license model), select the Unlimited check box. This allows as many connections as needed in the connection pools for DB Proxy and reporting.• 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 200, with a default of 10. Of the connections specified, ~75% are allocated to DB Proxy, ~25% for reporting, and 1 is unallocated for administrative purposes.
Username	The name used to access the QM database (see "Prerequisites" on page 22).
Password	The password used to access the QM database (see "Prerequisites" on page 22).

Enterprise Settings

The Enterprise Settings window (see [Figure 10](#)) enables you to:

- Enable automated software updates for client computers
- Configure Active Directory domains (in an Active Directory system only)
- View license information

Figure 10. Enterprise Settings window.



Automated Updates

If you enable automated updates, every time a client application is started, it checks the QM servers to determine if a newer version is available. If there is a newer version, it is automatically installed.

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 a domain you configure or on a trusted domain
- There must be at least one domain configured
- Each domain must have at least one user path configured

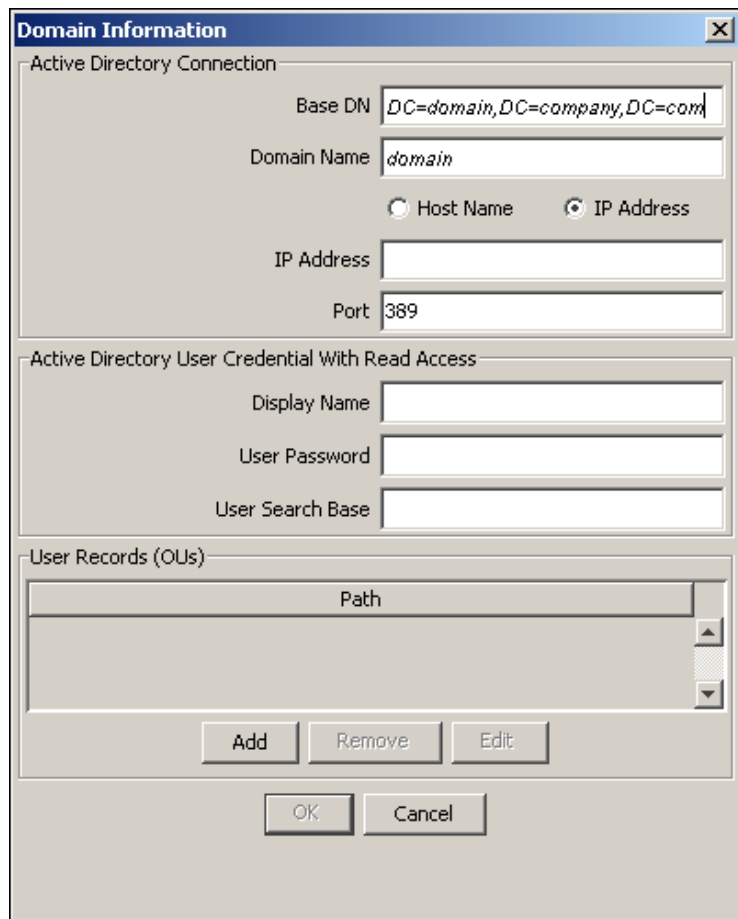
You can add, edit, and remove Active Directory domains.

To add an Active Directory domain:

1. Click **Add**.

The Domain Information dialog box appears (see [Figure 11](#)).

Figure 11. Domain Information dialog box.



2. Complete the dialog box 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 10. Domain Information dialog box fields.

Field	Description
Active Directory Connection	

Table 10. Domain Information dialog box fields.

Field	Description
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	
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.
Active Directory User Credential with Read Access	
Display Name	The name 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.
User Records (OUs)	<p>One or more paths to user records (OUs). Click Add to add at least one path, or Remove to remove an existing path. Maximum 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 Licensing section displays the bundle you have purchased.

Recording File Storage Location

Use this window 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.

- **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:** 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.

Figure 12. Recording Location window.

To change the recording location:

1. Select if you want to store recordings in a local or external storage location, and then enter or browse to the desired location in the Storage Location field.
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 <doman>\<username>.

This user meet these requirements:

- The user must be known to the local server (be a local user or 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.

3. Click **OK**.

Upload Settings

The Upload Settings window 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 13. Upload Settings window.

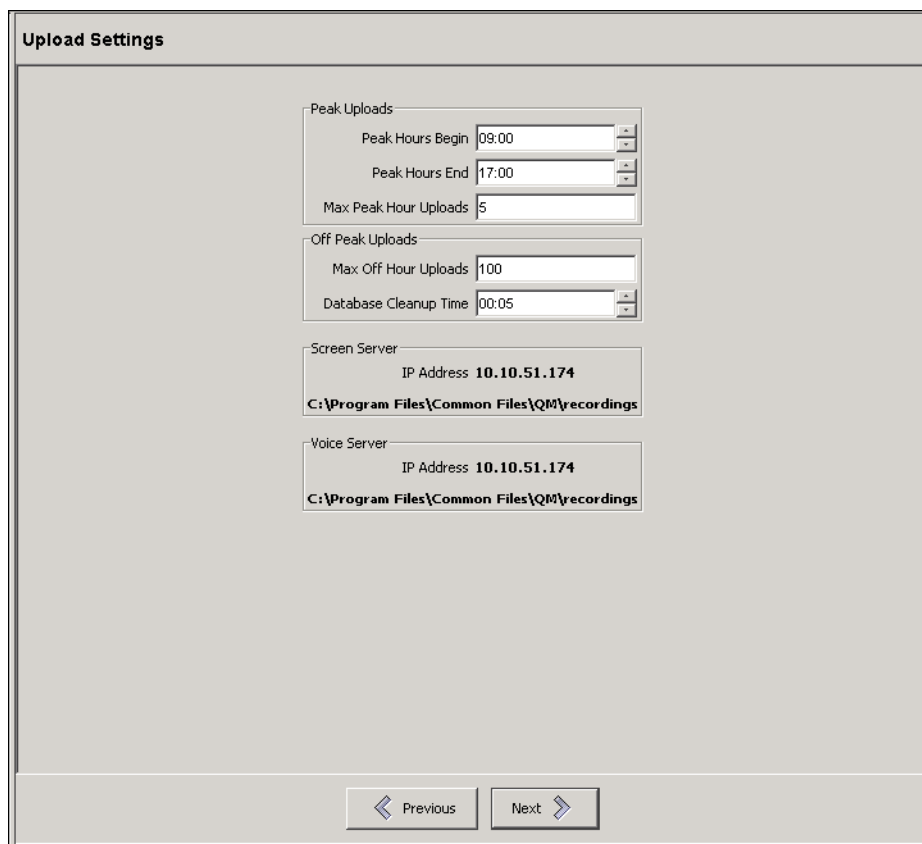


Table 11. Upload Settings fields

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.
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.

Table 11. Upload Settings 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.
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.
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.
Recording Servers (appears after the Voice service is installed)	
IP Address	The IP addresses of the machines that hosts the Voice and Screen services. If the Standard bundle is installed, only the Voice IP Address is listed.

Cisco Unified CM

The Cisco Unified CM window (see [Figure 14](#)) is used to configure the Cisco Unified CM cluster in your system, including information about the QM CTI service and Unified CM (JTAPI) user associated with the cluster.

Each 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.

Figure 14. CallManager Clusters window.

The screenshot shows the 'CallManager Clusters' configuration window. At the top, it displays 'Cluster: 1'. Below this, there are two main sections:

- QM CTI Service:**
 - Service Location:** Radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field contains '10.192.252.40'.
 - JTAPI User:** 'Username' field contains 'JTAPICCE1' and 'Password' field contains '*****'.
- CallManager Cluster:** A table with columns for 'Host Name', 'IP Address', 'Primary CTI Manager', and 'Backup CTI Manager'.

Host Name	IP Address	Primary CTI Manager	Backup CTI Manager
	192.168.252.66	<input checked="" type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input checked="" type="radio"/> None

At the bottom of the window, there are 'Previous' and 'Finish' navigation buttons.

Table 12. CallManager Clusters fields

Field	Description
QM CTI Service Location	
Host Name	The host name of the QM CTI service. This field appears only if the Host Name radio button is selected.
IP Address	The IP address of the QM CTI service. This field appears only if the IP Address radio button is selected.
Username	The JTAPI user name. This is the application user with which all phone devices are associated. This must be between 1 and 32 alphanumeric characters.
Password	The JTAPI user's password. This must be between 1 and 32 alphanumeric characters.
CallManager Cluster	
Host Name/ IP Address	The host name or IP address of the publisher and subscriber (if any) Cisco Unified CM, depending on which radio button is selected. You can enter 1 publisher Unified CM, and up to 8 subscriber Unified CMs.
Primary CTI Manager	Select this button if the Unified CM is the primary CTI Manager. There can be only one primary CTI Manager. Once entered, a primary CTI Manager may be reassigned, but not deleted.
Backup CTI Manager	Select this button if the Unified CM is the backup CTI Manager. There can be one or no backup CTI Manager.
None	Select this button if there is no backup CTI Manager. Default setting = selected.

QM JTAPI Installation

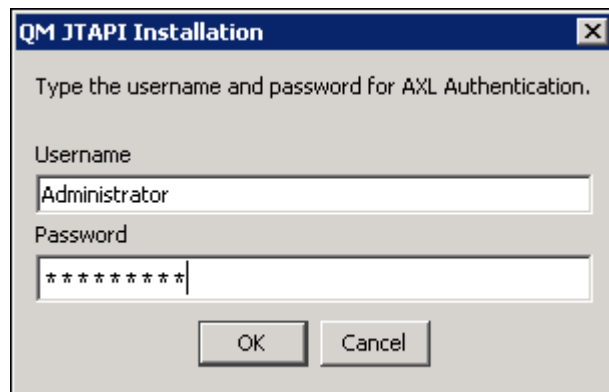
In CTI service installations, the QM JTAPI Installation dialog box appears. Enter the AXL (Administrative XML Layer) authentication username and password. These are configured when the Unified CM is set up.

QM Configuration Setup uses AXL to communicate with the Unified CM in order to discover the URL where the JTAPI plug-in is located. Once the location is known, Configuration Setup downloads and runs the JTAPI install for that version of Unified CM.

NOTE: If you upgrade your Unified CM you must also update the jtapi.jar on the QM CTI Services computer by using the

Download/Install JTAPI step from the Tools menu. If the JTAPI installation fails, uninstall the existing JTAPI version (Start > Program Files > CiscoJTAPI > Uninstall) and run the Download/Install JTAPI step again.

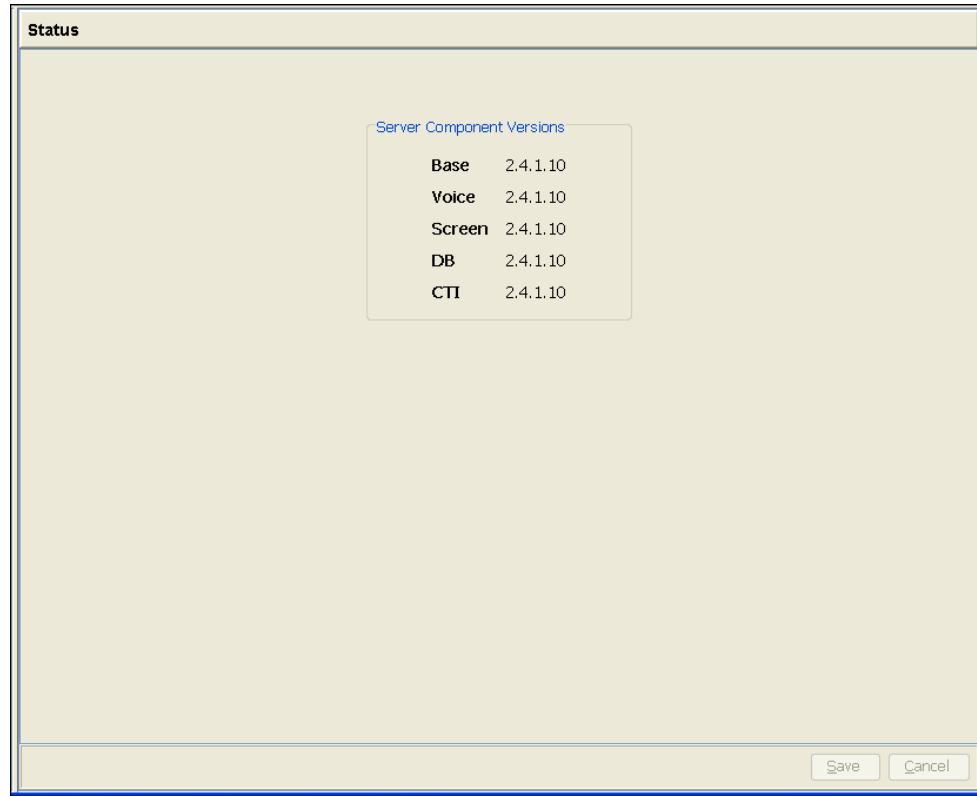
Figure 15. QM JTAPI Installation dialog box.



Status

The status window (see [Figure 16](#)) displays which version of each QM component is installed.

Figure 16. Status window.



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:

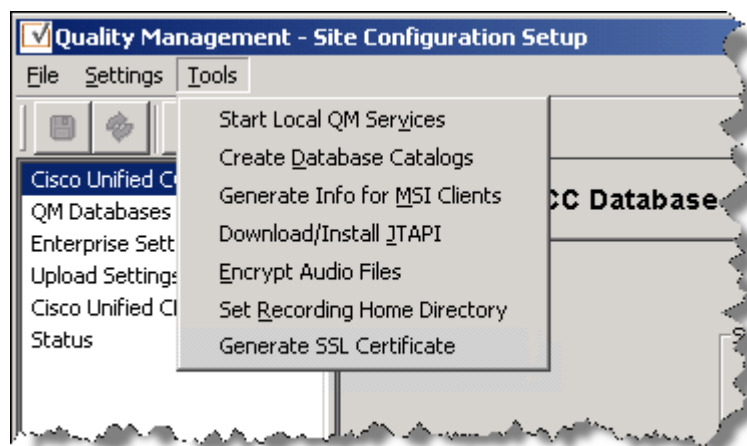
1. Start QM Configuration Setup.

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.

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 (see [Figure 17](#)). These tools normally run during the initial installation of QM.

Figure 17. QM Configuration Setup tools.



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 will ask for the AXL user name and password needed to access the upgraded Unified CM.

Encrypt Audio Files

Audio files were not encrypted in QM 2.1. They are encrypted in QM 2.4. When upgrading from version 2.1 to 2.4, 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 2.4. 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 36) so you can change the location where recordings are stored. This step must be run when upgrading from the Standard to the Enhanced bundle.

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.

Upgrading from Previous Versions

QM 2.4 can be installed over QM 2.3 (an “over the top” upgrade). Consult the release notes for any further notes on 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 (see [page 29](#)), 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. 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 ...\\Cisco\\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 51](#).

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.

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 (see [page 29](#)), 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 47](#).

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

1. On the computer that hosts Cisco Unified CCX , 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: If you attempt to install a QM application to a non-default location, the number of characters in the defined path cannot exceed that of the default installation location (25 characters, including spaces).

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>\QM\Tomcat\webapps\TUP\QM

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:

```
/!*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.

This is especially important for service release installations, which must be uninstalled before upgrading the underlying software.

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 55](#).
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.

Removing QM

3

Removing QM

Uninstall QM in the following order:

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\Comon Files\SQM\Recordings

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

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.

Index

A	Installing QM services prerequisites 22 procedure 25
Active Directory domain adding 34	
Automated package distribution tools 55	L
C	LDAP 9
CallManager Clusters window 40	M
D	Microsoft SQL Server 2005 firewall port exceptions 23 Microsoft SQL Server 2005 installation 22
DBCleaner service 8	
DBProxy service 8	
DBSync service 9	N
E	Named pipes 51 NT authentication 47
Elevated privileges 53	
Enterprise Settings window adding an Active Directory domain 34	P
F	Pushing desktop installations 55
File Transfer Servlet (FTS) 9	Q
Firewall port exceptions for Microsoft SQL Server 2005 23	QM Administrator about 8
I	QM components 8
Installation order 21	CTI service 8
Installing Microsoft SQL Server 2005 22	DBCleaner service 8
Installing QM desktop applications 53	DBProxy service 8
enabling elevated privileges 53	DBSync service 9
procedure 54	File Transfer Servlet (FTS) 9
using automated package distribution tools 55	LDAP 9
	QM Administrator 8
	QM Desktop 8
	QM Recording 8

- QM Configuration Setup 27
 - CallManager Clusters window 40
 - entering data in Initial Mode 27
 - entering data in Update Mode 43
 - QM JTAPI Installation dialog box 41
 - tools 44
- QM CTI service 8
- QM Desktop
 - about 8
- QM installation order 7
- QM Recording
 - about 8

R

- Removing QM applications and services 59

S

- Setting up named pipes 51
- Setting up NT authentication 47