



Cisco Unified Workforce Optimization

Quality Management Administrator User 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 Administrator User Guide

© 2008 Cisco Systems, Inc. All rights reserved.

© 2008 Calabrio, Inc. All rights reserved.

Contents

Overview 7

- What's New In This Version 7
- Quality Management API 8
- Logging In to QM Administrator 9
- Changing Your Password 10
- Synchronizing Databases 11
- Logging Out of QM Administrator 12
- Automated Updates 13
- The QM Administrator Interface 14
 - Moving Within the Navigation Tree 14
 - Mouse 14
 - Keyboard 14
 - Sorting Tables 15

Site Configuration 17

- Introduction 17
- Modifying Site Configuration Information 18
- Site Configuration Windows 19
 - Cisco Unified CC Database 19
 - Cisco Unified CM 21
 - QM Databases 23
 - QM CTI Service 25
 - Enterprise Settings 26
 - Software Updates 27
 - Session Timeout Options 27
 - Licenses 27
 - Active Directory 27
 - Locale 30
 - Upload Settings 31
 - Monitoring and Notification 33
 - Configuring Email Addresses for Notification 36

Contents

Configuring Notification Triggers	39
Examples of Notification Problem Configuration	43
CDR Information Formats	44
Inclusion List	46
Excluding Extensions	47
Status	49

Record Server Configuration 51

- Introduction 51
- Mobile Agent Monitor 52
- VoIP Devices 54

Personnel 59

- Introduction 59
- User Roles and Privileges 60
 - Agents and Knowledge Workers 60
 - Supervisors 60
 - Managers 60
 - Archive Users 61
 - Evaluators 61
- User Administration 62
 - Active Directory Systems 62
 - Linking ACD Users to AD Users 64
 - Bulk Linking 64
 - Individual Linking 65
 - Switching AD-ACD Links 67
 - Deleting an ACD User 67
 - Creating a QM User 67
 - Non-Active Directory Systems 69
 - Configuring an ACD User 71

Contents

- Unconfiguring or Deleting an ACD User 72
- Creating a QM User 72
- Assigning Roles to a QM User 73
- Licensing Users 73
- Team Administration 75
- Group Administration 77
 - Adding a New Group 77
 - Assigning Teams and Managers to a Group 78
 - Removing Teams and Managers From a Group 80
 - Renaming a Group 80
 - Deleting a Group 80

Recordings 83

- Introduction 83
 - About Recordings 83
 - About User-Defined Metadata 84
- Configuring Recording Retention Periods 85
 - Quality Management Recordings 85
 - Archive Recordings 87
- Enabling Recording Export 89
- Configuring User-Defined Metadata 90
- Creating a Workflow 93
 - How Multiple Classifiers in a Workflow are Executed 93
 - Example 93
 - Creating a New Workflow 95
 - Setting Up Classifiers 96
 - Configuring Actions 98
 - Setting Up Rules 99
 - Modifying or Deleting a Workflow 103

Contents

Evaluation Forms 105

- Introduction 105
 - Form Status 106
 - Creating an Evaluation Form 107
 - Creating a New Evaluation Form 108
 - Properties Tab 109
 - Header Tab 111
 - Sections Tab 111
 - Questions Tab 113
 - Key Performance Indicator (KPI) Questions 114
-

Backup and Restore 115

- Introduction 115
 - Upgrades 115
 - Disaster Recovery 115
 - BARS and Cisco Security Agent 116
 - Command Line Syntax 116
 - Backing Up the LDAP and QM Databases 116
 - Restoring the LDAP and QM Databases 117
-

Index 119

What's New In This Version

This version of Quality Management (QM) Administrator includes these new features:

- Recording supported for Cisco Mobile Agents (audio and video), thin client agents using Citrix or Windows Terminal Services (audio only), and agents who use phones without PCs (audio only)
- Voice and screen recordings can now be exported in standard movie file format (WMV)
- Evaluation approval on the form level for specified roles
- Session timeouts for QM Desktop, QM Administrator, and reports
- Archiving at the team level
- 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

Quality Management API

The Quality Management (QM) API provides a means for users to create an external application that enables agents to perform the following tasks:

- Tag calls for retention
- Delete recordings
- Attach user-defined metadata to calls
- Export a recording based on its ID or metadata
- Search for a recording
- Edit metadata associated with a recording
- Pause voice and screen recording

The QM Recording Client enables the API by accepting formatted requests passed via sockets to an IP address and port.

The QM API can be integrated with the Cisco Agent Desktop (CAD) interprocess communication (IPC) action. IPC actions pass information in the form of user datagram protocol (UDP) messages from the agent desktop to a third-party application (in this case, the QM API) using IPC methods.

See "[Configuring User-Defined Metadata](#)" on [page 90](#) for information on configuring metadata for use with the QM API. See the *Quality Management API Programmers Guide* for information on using the QM API.

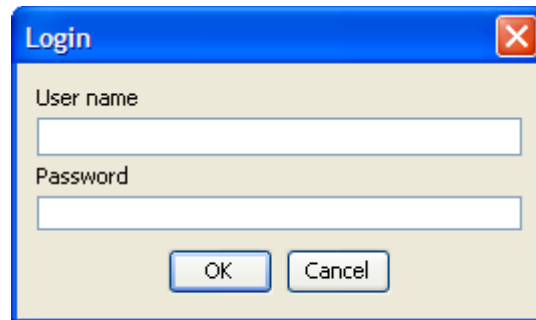
Logging In to QM Administrator

To log in to QM Administrator:

1. Choose Start > All Programs > Cisco > WFO > Quality Management Administrator.

QM Administrator starts and the Login dialog box appears (Figure 1).

Figure 1. Login dialog box



2. Complete the dialog box as follows, and then click OK or press Enter.
 - Enter Administrator in the User name field. This is the default setting and cannot be changed. This field is not case sensitive.
 - Enter the password set up during system installation in the Password field. This field is case sensitive.

NOTE: Only one user can log in to QM Administrator at a time. If another user is logged in, you will not be able to log in.

3. QM Administrator will validate your login against the user and password set up during system installation, and then log you in.

Changing Your Password

Passwords should remain confidential. If the QM Administrator password becomes known, follow these steps to change it.

To change the QM Administrator password:

1. From the menu bar, choose Settings > Change Administrator Password.
The Change QM Administrator Password dialog box is displayed (Figure 2).

Figure 2. Change QM Administrator Password dialog box



The image shows a standard Windows-style dialog box titled "Change QM Administrator Password". It features a blue title bar with a red close button in the top right corner. The main area is light beige and contains three text input fields stacked vertically, labeled "Old password", "New password", and "Confirm new password". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

2. Enter your old password, a new password, and the new password again to confirm it.
The password must be between 1 and 32 alphanumeric characters long. It is case sensitive.
3. Click OK.

Synchronizing Databases

Teams, agents, and supervisors are set up in Cisco Unified Contact Center Express (Unified CCX). This information must be made available to QM, so the Unified CCX and QM databases are synchronized automatically at 10-minute intervals.

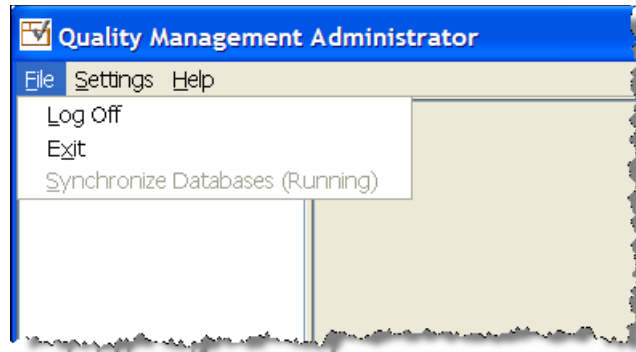
You can manually synchronize the databases if necessary.

To manually synchronize the databases:

1. On the menu bar, choose File > Synchronize Databases.

The synchronization process starts. While the process is running, the menu option changes from Synchronize Databases to Synchronize Databases (Running) and is disabled (Figure 3).

Figure 3. The Synchronization Databases option while sync is in progress



2. When the process is complete, the menu option changes back to Synchronize Databases and is enabled.

Logging Out of QM Administrator

There are two ways of logging out of QM Administrator:

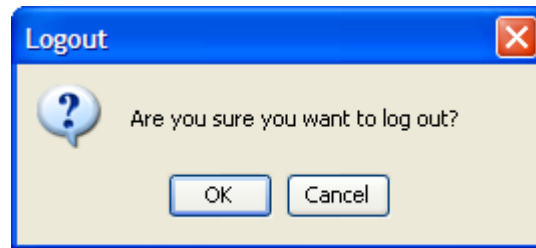
- Logging out and leaving QM Administrator running
- Logging out and closing QM Administrator

To log out and leave QM Administrator running:

1. From the menu bar, choose File > Log Off.

The logout confirmation dialog box appears ([Figure 4](#)).

Figure 4. Logout confirmation dialog box



2. Click OK.

To log out and close QM Administrator:

- From the menu bar, choose File > Exit, or click the Close button in the upper right corner of the window.

Automated Updates

Quality Management can be configured to enable automated updates. This means that whenever a newer version of QM is installed on the servers, all instances of the client applications (QM Administrator, QM Desktop, and QM Desktop Recording) will also be updated.

With automated updates enabled, every time you start QM Administrator it checks to see if there is an updated version available. If there is, it automatically runs the update process.

NOTE: If the automated update process is running, do not attempt to start any of the QM desktop applications, or another instance of the automated update process may start.

When this happens, you will see a dialog box notifying you that your instance of QM Administrator will be updated. Click OK and then follow the instructions in the installation wizard that follows.

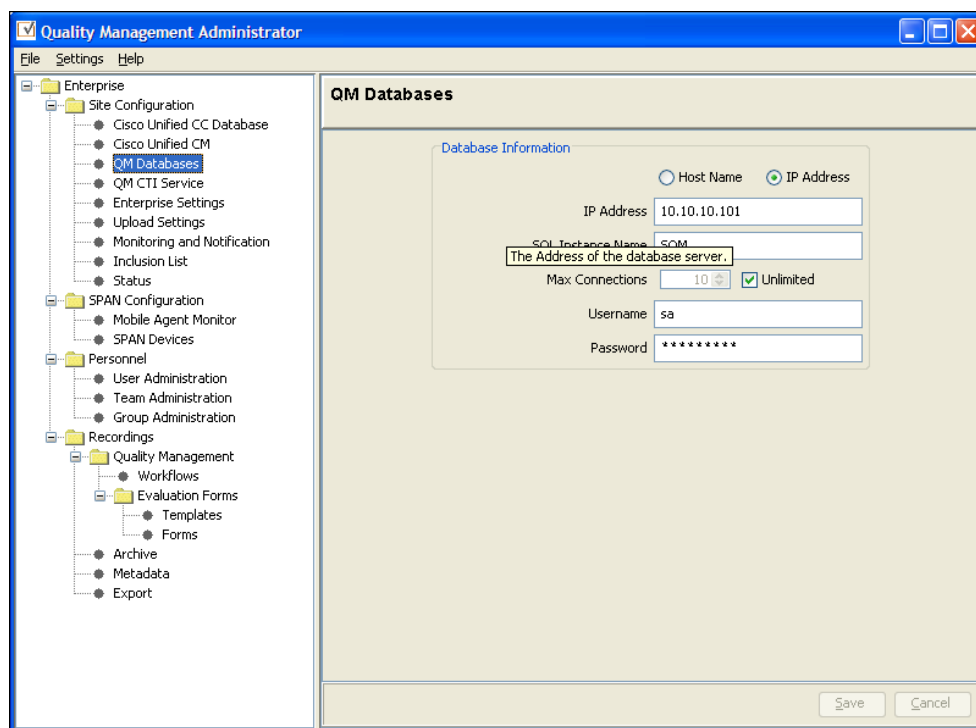
When the update is finished, you will see a final dialog box telling you that your update is complete. Click OK, and then restart QM Administrator and log in as usual.

NOTE: If you cancel an update, the update will fail. However, you will still see a message that the upgrade has completed.

The QM Administrator Interface

The QM Administrator interface (Figure 5) has two panes. The left pane is a navigation tree. The right pane displays the node you select in the left pane.

Figure 5. QM Administrator interface



Moving Within the Navigation Tree

Use these mouse or keyboard actions to move within the navigation tree.

Mouse

- Double-click an icon/node name to expand or collapse the tree.
- Click the plus sign (+) to expand the tree.
- Click the minus sign (-) to collapse the tree.

Keyboard

- Press the up and down arrow keys to move from one node to the next.
- Press the left arrow key to collapse the tree.
- Press the right arrow key to expand the tree.

Sorting Tables

Data that is presented in table form (Figure 6) can be sorted by as many columns as there are in the table. The sort can be ascending or descending.

The small triangles at the right of the column header display the direction of the sort, ascending or descending. These arrows also change size depending on the column's position in the sort. The triangle in the primary sort column is biggest, the one in the secondary sort column is slightly smaller, and so on.

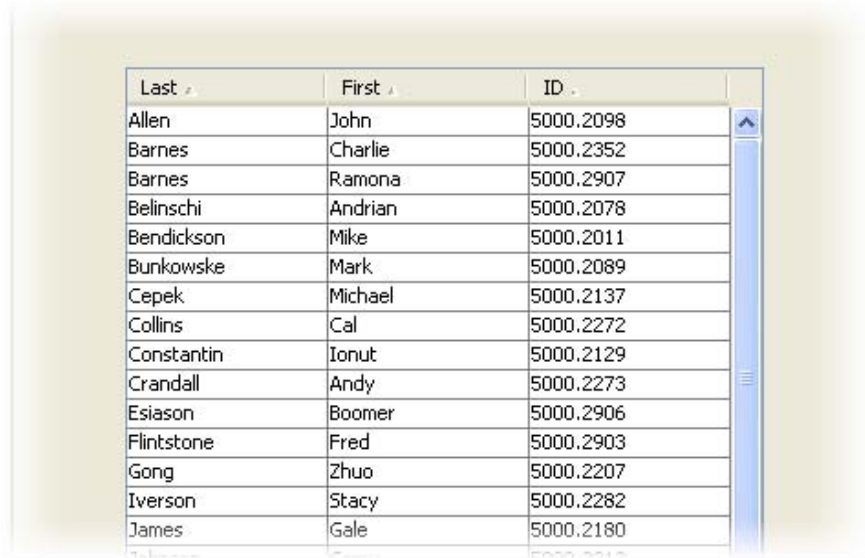
To sort a table by one column:

- Click on the column header. Click again to reverse the sort order.

To sort a table by multiple columns:

1. Ctrl + Click the primary sort column header.
2. Continue holding down the Ctrl key and then click any other column headers you want to sort the table by.

Figure 6. Example of a sortable table



Last ▲	First ▲	ID ▲
Allen	John	5000.2098
Barnes	Charlie	5000.2352
Barnes	Ramona	5000.2907
Belinschi	Andrian	5000.2078
Bendickson	Mike	5000.2011
Bunkowske	Mark	5000.2089
Ceppek	Michael	5000.2137
Collins	Cal	5000.2272
Constantin	Ionut	5000.2129
Crandall	Andy	5000.2273
Esiason	Boomer	5000.2906
Flintstone	Fred	5000.2903
Gong	Zhuo	5000.2207
Iverson	Stacy	5000.2282
James	Gale	5000.2180

Introduction

Site configuration information is initially entered in the QM Site Configuration Setup utility (PostInstall.exe), which runs automatically after services are installed.

After this initial installation, the information can be changed using QM Administrator's Site Configuration node.

The Site Configuration windows are:

- [Cisco Unified CC Database \(page 19\)](#)
- [Cisco Unified CM \(page 21\)](#)
- [QM Databases \(page 23\)](#)
- [QM CTI Service \(page 25\)](#)
- [Enterprise Settings \(page 26\)](#)
- [Upload Settings \(page 31\)](#)
- [Monitoring and Notification \(page 33\)](#)
- [Inclusion List \(page 46\)](#)
- [Status \(page 49\)](#)

Modifying Site Configuration Information

To modify the site configuration information, follow this procedure.

Modifying site configuration information:

1. Expand the Site Configuration node in the navigation tree, and then select the window you wish to modify.

The selected window appears in the right pane.

2. Enter the new data in the appropriate fields.
3. Click Save.

Modifications must be saved in order to take effect.

Site Configuration Windows

Cisco Unified CC Database

The Cisco Unified CC Database window (Figure 7) is used to configure access to and identify the location of the Cisco Unified Contact Center Express database.

Figure 7. Cisco Unified CC Database window

The screenshot shows the 'Cisco Unified CC Database' configuration window. It features a title bar with the text 'Cisco Unified CC Database'. Below the title bar is a note: 'Note: This information is only editable on the Base Server.' The window is divided into several sections:

- Side A:** Contains radio buttons for 'Host Name' and 'IP Address', with 'IP Address' selected. Below is a text box for 'IP Address' containing the value '10.192.252.21'.
- Side B:** Contains radio buttons for 'Host Name' and 'IP Address', with 'IP Address' selected. Below is an empty text box for 'IP Address'.
- ICM Instance Name:** A text box containing the value 'rd21'.
- Authentication:** Contains radio buttons for 'SQL' and 'NT', with 'SQL' selected. Below are text boxes for 'Login ID' containing 'sa' and 'Password' containing '*****'.
- Connection:** Contains radio buttons for 'TCP/IP' and 'Named Pipe', with 'TCP/IP' selected. Below is a text box for 'Port' containing the value '1433'.

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

The information in this window can be edited only if you use the QM Configuration Setup utility (PostInstall.exe) on the machine that hosts the QM base services. When viewed in QM Administrator, it is read-only.

NOTE: For more information on the QM Configuration Setup utility, see “QM Configuration Setup” in the *Quality Management Installation Guide*.

In order for any changes you make in QM Configuration Setup to take effect, you must restart the Sync service.

Table 1. Cisco Unified CC Database fields

Field	Description
Side A IP Address/ Host Name	The IP address or host name of the Side A (primary) Cisco Unified CC database.
Side B IP Address/ Host Name	The IP address or host name of the Side B (secondary) redundant Cisco Unified CC database, if one exists.
SQL Instance Name	The SQL instance name.
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" in the <i>QM Installation Guide</i> . Default = NT. 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.
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" in the <i>QM Installation Guide</i> .
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 window (Figure 8) is used to configure the Cisco Unified Communications Manager 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 window

The screenshot shows the 'Cisco Unified CM' configuration window. At the top, it displays 'Cluster: 1'. Below this, there are two main sections: 'SOAP AXL Access' and 'JTAPI User'. The 'SOAP AXL Access' section has a 'Username' field with 'administrator' and a 'Password' field with '*****'. The 'JTAPI User' section has a 'Username' field with 'bunkowmjtapi' and a 'Password' field with '*****'. Below these is the 'Cisco Unified Communications Manager Cluster' section. It features a 'Publisher' section with radio buttons for 'Host Name' and 'IP Address' (selected), and a text input field containing '10.192.252.74'. To the right of the 'Publisher' section are radio buttons for 'Primary CTI Manager' and 'Backup CTI Manager'. A 'Find Subscribers' button is located below the 'Publisher' section. The 'Subscribers' section contains a table with columns for 'Host Name', 'IP Address', 'Primary CTI Manager', and 'Backup CTI Manager'. Each column has radio buttons. At the bottom right of the 'Subscribers' section is a 'None' option. At the very bottom of the window are 'Previous' and 'Next' navigation buttons.

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 2. Cisco Unified CM step fields

Field	Description
SOAP AXL Access	
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.
JTAPI User	
Username	The JTAPI user name. This is the application user with which all phone devices used for recording are associated. The QM CTI service logs into the Unified CM with this user. The user name must be between 1 and 32 alphanumeric characters.
Password	The JTAPI user's password. This must be between 1 and 32 alphanumeric characters.
Cisco Unified Communications Manager Cluster	
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 window

In order for any changes you make to take effect, you must restart the DbProxy service.

Table 3. QM Database 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 3. QM Database fields (cont'd)

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 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.
Unlimited	Used in conjunction with Max Connections. See that description for more information.
Username	The name used by the QM DBProxy service to access the QM database (see "Prerequisites" in the <i>QM Installation Guide</i> for more information).
Password	The password used to access the QM database (see "Prerequisites" in the <i>QM Installation Guide</i> for more information).

QM CTI Service

The QM CTI Service window (Figure 10) is used to configure the location of the QM CTI service.

Figure 10. QM CTI Service window

Table 4. QM CTI Service fields

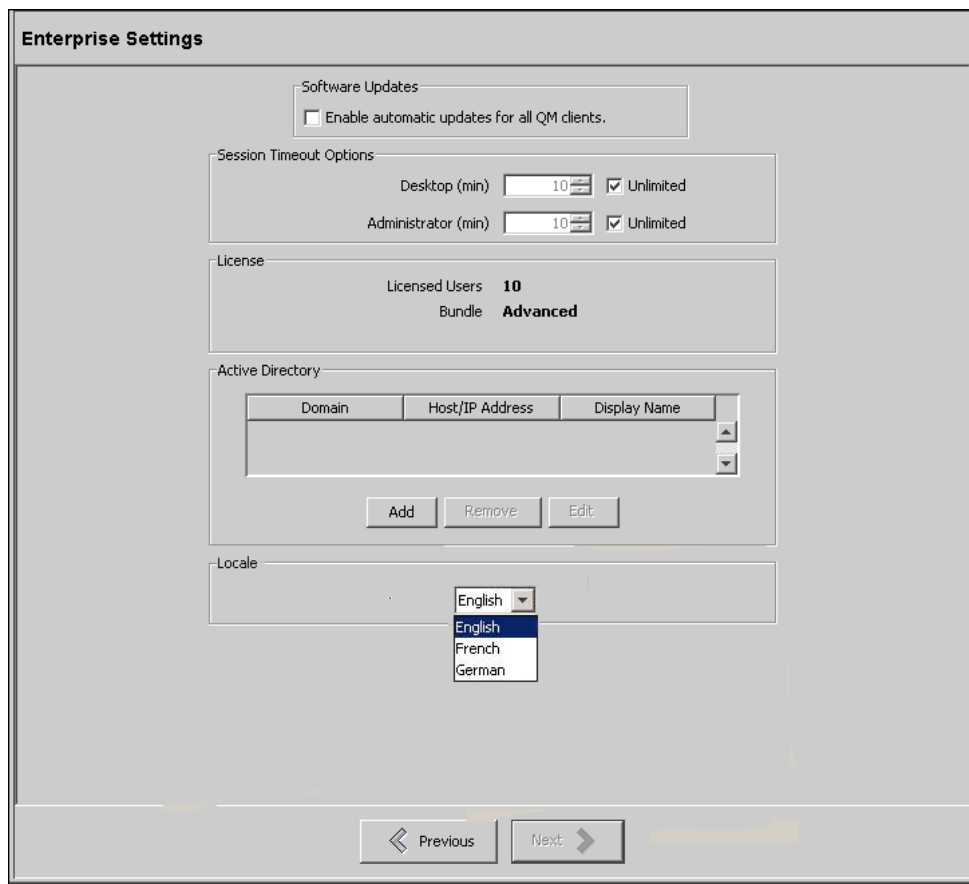
Field	Description
Cluster	(Read only) The IP address of the Cisco Unified Communications Manager cluster to which the CTI service will connect for call events.
Host Name/IP Address	The host name or IP address of the QM CTI service.

Enterprise Settings

The Enterprise Settings window (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

Figure 11. Enterprise Settings window



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

If you enable automated updates for all QM clients, 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 on the client desktop.

NOTE: If you apply a service release (SR) update to the system, it is recommended that you disable the automated update feature first. After the SR update is installed, manually test an updated instance of QM Recording, QM Desktop, and QM Administrator to verify they work. When you are satisfied they work, you can re-enable the automated update feature.

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.

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.

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

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 a 'Domain Information' dialog box with the following sections and fields:

- Active Directory Connection:**
 - Base DN: DC=rndcc2,DC=acmi,DC=com
 - Domain Name: rndcc2
 - Radio buttons: Host Name, IP Address
 - Host Name: rndcc2.acmi.com
 - Port: 389
- Active Directory User Credential With Read Access:**
 - Display Name: administrator
 - User Password: *****
 - User Search Base: cn=Users
- User Records (OUs):**
 - Path list:
 - ou=Users,ou=Minneapolis,ou=Minnesota,ou=US
 - ou=Users,ou=StPaul,ou=Minnesota,ou=US
 - Buttons: Add, Remove, Edit
- Bottom Buttons:** OK, Cancel

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 5. Domain Information dialog box fields

Field	Description
Active Directory Connection	
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.
Active Directory User Credential with Read Access	
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 5. Domain Information dialog box fields (cont'd)

Field	Description
User Records (OUs)	<p>One or more paths to user records (OUs). Click Add to add at least one path, or Remove to remove an existing path. Maximum 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.

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.

Upload Settings

The Upload Settings window (Figure 13) is used to schedule uploading of peak and off-peak recordings from the agent desktops to the audio and screen servers, as well as recording metadata to the QM database.

Figure 13. Upload Settings window

The screenshot shows the 'Upload Settings' window with the following configuration:

- Peak Uploads:**
 - Peak Hours Begin: 09:00
 - Peak Hours End: 17:00
 - Max Peak Hour Uploads: 5
- Off Peak Uploads:**
 - Max Off Hour Uploads: 100
 - Database Cleanup Time: 00:05
- Screen Server:**
 - IP Address: 10.10.51.82
 - Path: C:\Program Files\Common Files\QM\recordings
- Voice Server:**
 - IP Address: 10.10.51.82
 - Path: C:\Program Files\Common Files\QM\recordings

Navigation buttons: Previous (left arrow) and Next (right arrow).

NOTE: Recordings for deactivated agents cannot be uploaded. When an agent is deleted from the ACD, it is recommended that you ensure there are no recordings for that agent still on the agent PC in either the Daily or Staging folders. After all recordings for that agent have been uploaded, it is safe to delete the agent from the ACD.

In order for any changes you make (except Database Cleanup Time) to take effect, you must restart the Upload Controller service.

Table 6. 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. Default = 09:00.
Peak Hours End	The time, in 24-hour format, when peak hours in the contact center end. Must be between 00:00 and 23:59 in 1-minute increments. Default = 17:00.
Max Peak Hour Uploads	The maximum number of recordings that can 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. Default = 00:05.
Screen Server IP Address	(Read-only) The IP address of the machine that hosts the Screen services and video recordings, and the path where video recordings are stored.
Voice Server IP Address	(Read-only) The IP address of the machine that hosts the Voice services and audio recordings, and the path where audio recordings are stored.

Monitoring and Notification

The Monitoring and Notifications window (Figure 14) 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
- If and how often a renotification of the problem should be sent out
- Types of problems that will trigger notification

Figure 14. Monitoring and Notifications window

Monitoring and Notification

Use Monitoring/Notification Service

Notification

Use Event Viewer Notification

Use SNMP Notification *

Use Email Notification *

Email Addresses

Properties

Polling Period (in min)

Renotification Period

Never

Every 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

Changes made in this window take effect at the next polling diagnostic. If the Monitoring and Notification service is not enabled, it updates its configuration every 10 minutes.

If you enable the Monitoring and Notification service after the service has started, it performs its first diagnostic within 10 minutes.

Table 7. Monitoring and Notification window 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.
Properties	
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.
Notification	
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.
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 "Configuring Email Addresses for Notification" on page 36 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.
Renotification Period	
Never	Choose this option if you do not want to be renotified of a problem after the initial notification.

Table 7. Monitoring and Notification window fields (cont'd)

Field	Description
Every N Polling Periods	Choose this option and enter how frequently you want renotification to occur after the initial notification.
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 "Configuring Notification Triggers" on page 39 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 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, INFO and higher error 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.

The SNMP service can be installed using the Add/Remove Windows Components button in the Add or Remove Programs utility in Control Panel. Select Management and Monitoring Tools from the list of available components, and then choose Simple Network Management Protocol.

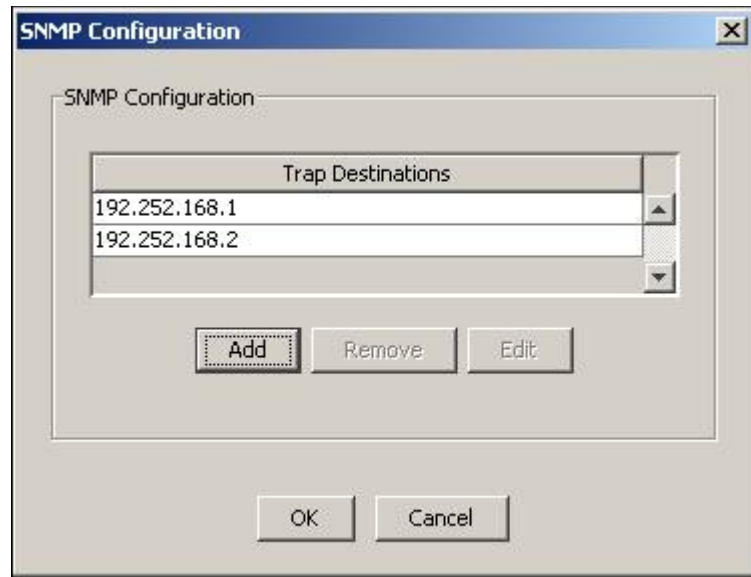
SNMP allows you to monitor and manage a network from a single workstation or several workstations, called SNMP managers. SNMP is actually a family of specifications that provide a means for collecting network management data from the devices residing in a network. It also provides a method for those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

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

To configure the SNMP settings:

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

Figure 15. 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 SNMP service to enable your changes.

Configuring Email Addresses for Notification

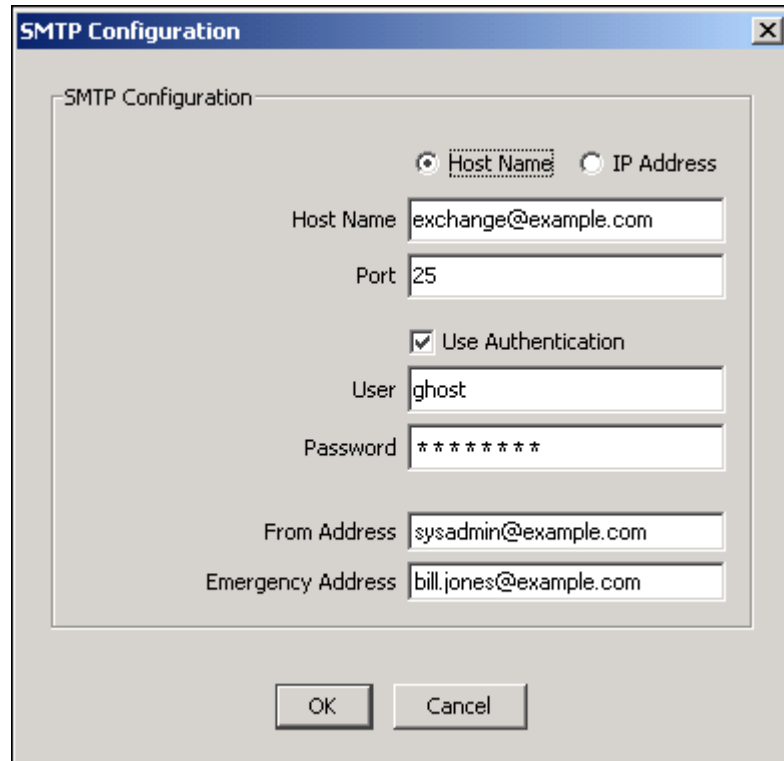
Notifications can be sent to either the Event Viewer or in emails to specified recipients. To use email notification, enable the Use Email Notification check box and then configure up to 5 email addresses.

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. On the Base Services server, start QM Administrator or QM Configuration Setup (PostInstall.exe).
2. Navigate to the Monitoring and Notification window.
3. Click SMTP Configuration. The SMTP Configuration dialog box appears (Figure 16).

Figure 16. SMTP Configuration dialog box



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

Table 8. 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.

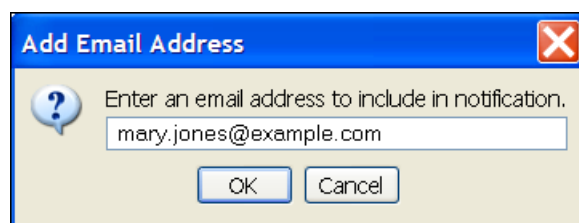
Table 8. SMTP dialog box fields (cont'd)

Field	Description
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.
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 17).

Figure 17. 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 Triggers

Currently, only one notification trigger requires configuration: Problem ID QM3002. This trigger compares data in the Cisco Unified Communications Manager's (Unified CM) Call Detail Record database (for Unified CM version 4.0) or CAR Report (for Unified CM versions 5.0 and 6.0) 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 notification trigger 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 trigger are:

- CDR is correctly configured in the Unified CM Administration web application.
 - Unified CM 4.0: 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 5.0 and 6.0: 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 trigger:

1. Click Notification Trigger Configuration. The Configuration dialog box appears (Figure 18).
2. Complete the fields as follows, and then click OK.

Table 9. Notification Trigger Configuration fields

Field	Description
CDR Configuration	

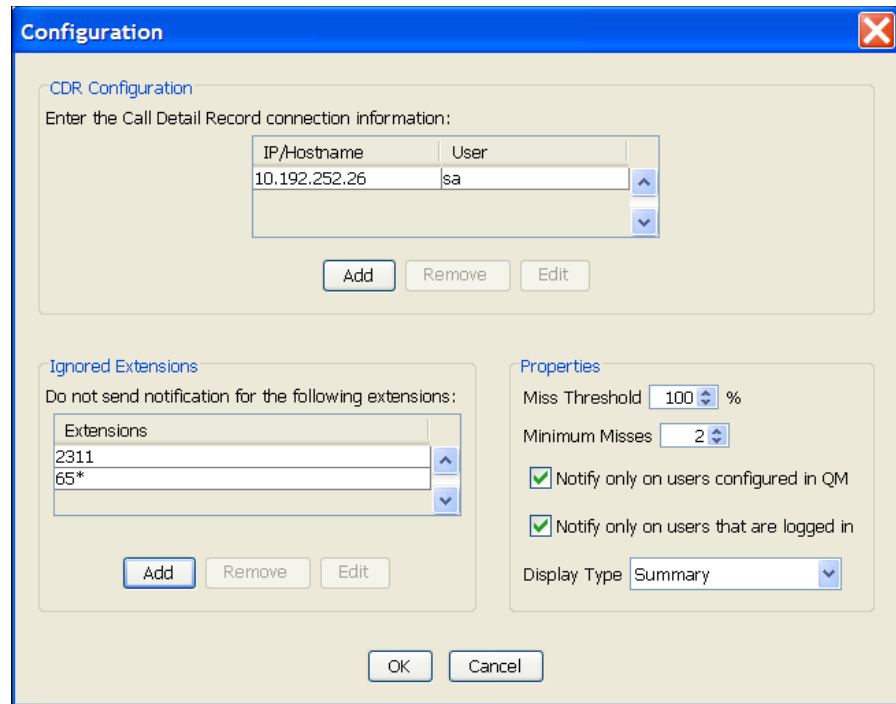
Table 9. Notification Trigger Configuration fields (cont'd)

Field	Description
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.
Ignored Extensions	
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.
Properties	
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.
Notify on users who are logged in	Enable this check box to trigger notification on only those QM users who are currently logged in. Default = Enabled.

Table 9. Notification Trigger Configuration fields (cont'd)

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"> • Summary Only • Detail (Tab Delimited) • Detail (Plain Text) <p>See "CDR Information Formats" on page 44 for more information.</p>

Figure 18. 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 19).

Figure 19. CDR Information dialog box

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

Table 10. 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	The instance name of the Unified CM database. Usually the default instance of the CDR database is used, so this field can be blank.
Username	The name of the user with rights to access the Unified CM database.
Password	The password of the user with rights to access the Unified CM database.

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 Problem Configuration

The following illustrate what happens when Notification Problem 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.

NOTE: Agent team association and whether a team is an archive team are determined for the time the CDR task is run, not for the time of the call in question. This could result in either false positives or false negatives if a team's archiving status changes, or if an agent's team membership changes during the period the CDR task is examining.

When a notification is received, look at the DNs/Agents that show missed calls. A large number of agents with missed calls might indicate a 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 Triggers" on page 39](#)). Examples of the available formats are listed here.

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

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

Inclusion List

The Inclusion List window (Figure 20) is used to configure a list of extensions to record for each Unified CM cluster. Only extensions in this list will be recorded.

Figure 20. Inclusion List window

Extension	<input checked="" type="checkbox"/> Inbound	<input type="checkbox"/> Outbound
12*	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13*	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Extension
1574
22*

By default, the inclusion list displays an asterisk (*) with both Inbound and Outbound check boxes selected, meaning that all incoming and outgoing calls on all extensions in that Unified CM cluster will be recorded.

As soon as specific extensions are configured, recording is limited to those extensions only. You can use the wild cards “?” and “*” to configure ranges of extensions.

- “*” in a string can represent any quantity of any character, as long as the other characters in the string match.

- “?” in a string can be replaced by any character, but the length of the string must be exactly as represented.

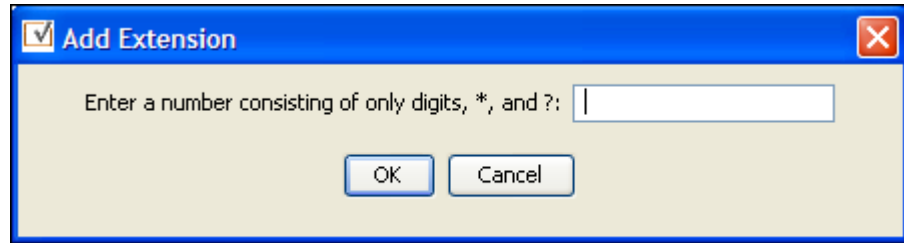
Extensions can be further filtered by selecting the Inbound and/or Outbound check boxes to limit recordings to calls going in a specific direction. At least one of these check boxes must be selected for each extension you enter. Any changes you make to the inclusion lists take effect at the next recording client login.

To add an extension to the inclusion list:

1. On the appropriate Unified CM cluster tab of the Inclusion List window, click Add.

The Add Extension dialog box appears (Figure 21).

Figure 21. Add Extension dialog box



2. Enter an extension number, and then click OK.

You can enter the exact extension number or use the * or ? wild card plus numbers to configure a range of extensions. For example:

Enter This:	To Record:
6124	Extension 6124
61*	Any extensions that start with 61 and are of any length (for example, 6124, 61555, 613)
61??	Any extensions that start with 61 and are 4 digits long (for example, 6124, 6125, 6126)

Excluding Extensions

If you have a limited number of extensions you want to exclude from being recorded, you can configure the inclusion list to ignore only those extensions and record all others.

For example, if you want to record all extensions except for extensions 3411, 3412, and 3413, configure your inclusion list so that there is an asterisk in the Extensions To

Be Recorded pane, and extensions 3411, 3412, and 3413 listed in the Extension To Be Excluded From Recording pane.

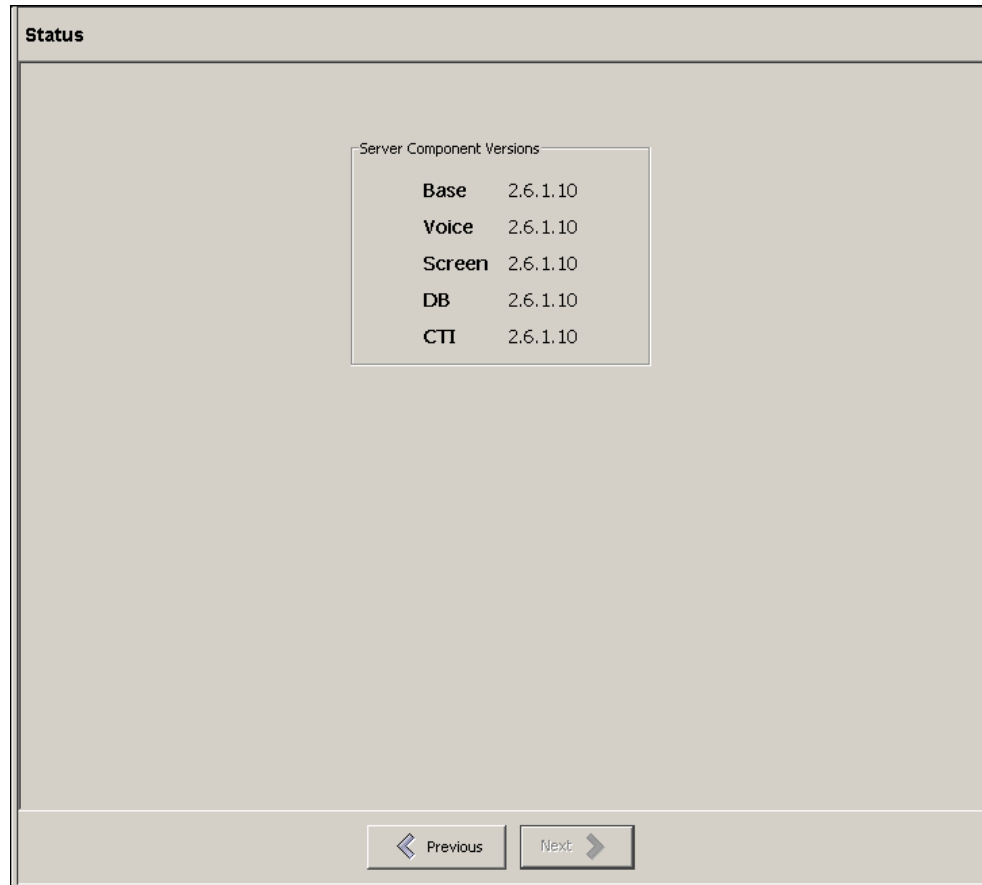
Extensions listed in the Extensions To Be Excluded From Recording pane always take precedence over extensions listed in the Extensions To Be Recorded pane. You cannot list the same extension (specifically or through the use of wild cards) in both panes. For example, **12*** cannot be listed in both panes.

Status

The Status window (Figure 22) reports the version of the installed QM components.

In a multi-server environment, this window also reports if a component has not yet been installed or if it needs to be upgraded.

Figure 22. Status window



Record Server Configuration

3

Introduction

The Record Server Configuration node is used to configure the mapping between agent gateways and QM Monitor service servers. This enables server-based recording for the following types of agents:

- Agents using Cisco Mobile Agent (audio and video recording)
- Agents using Citrix or Microsoft Terminal Services thin clients (audio recording only)
- Agents using just a phone, and no PC (audio recording only)

The extensions you configure for server-based recording are recorded in a similar way to those that use the QM Desktop Recording client (endpoint recording). Note that server-based recording is not restricted to the time a user is logged in. As long as the agent's phone device is configured for server-based recording, the agent can be recorded.

Server-based recording has the following limitations:

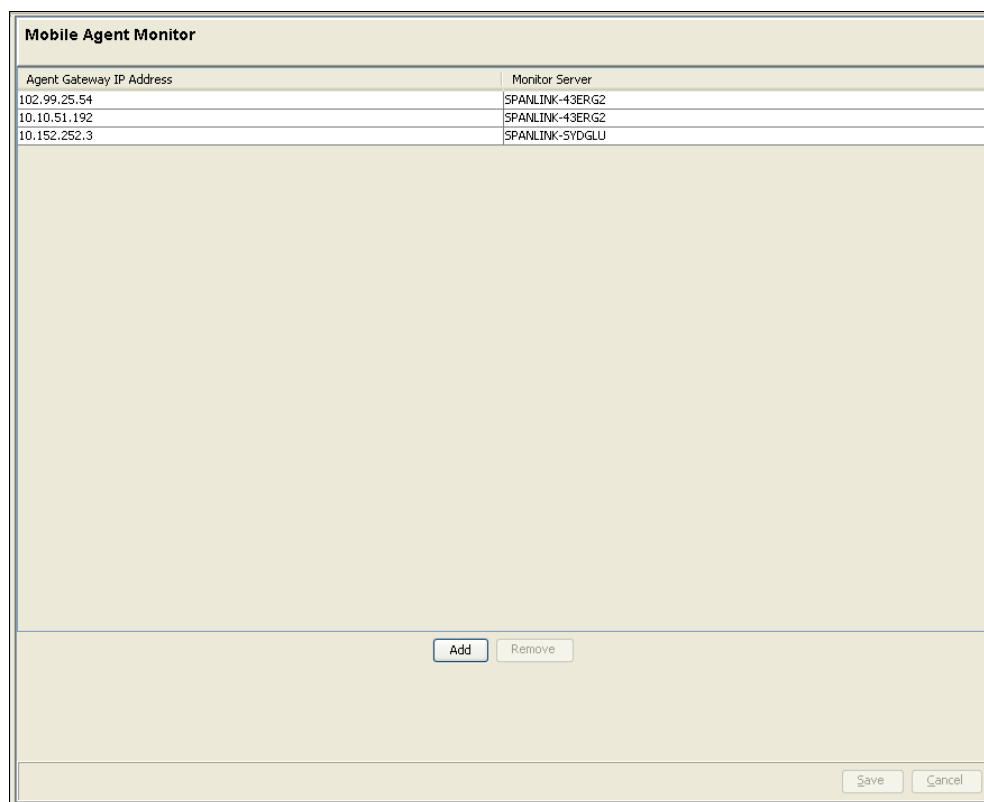
- a. if agents use the same extension (for example, two agents on different shifts use the same phone) all calls are attributed to the agent who is associated with that phone extension.
- b. Server-based recording does not support extension mobility.

Mobile Agent Monitor

The Mobile Agent Monitor window (Figure 23) is used to configure the mapping between agent gateways and QM Monitor service servers. It is used only if your system includes agents who use Cisco Mobile Agent. If your system does not include this type of agent, this window can be left blank.

The window displays two columns, one containing the agent gateway IP address and the other a drop-down list of available QM Monitor servers.

Figure 23. Mobile Agent Monitor window



Agent Gateway IP Address	Monitor Server
102.99.25.54	SPANLINK-43ERG2
10.10.51.192	SPANLINK-43ERG2
10.152.252.3	SPANLINK-SYDGLU

Buttons: Add, Remove, Save, Cancel

To add an agent gateway/Monitor server relationship:

1. In the Mobile Agent Monitor window, click Add. A row is added to the table.
2. In the Agent Gateway IP Address column, enter the IP address of an agent gateway.
3. In the Monitor Server column, select the appropriate Monitor server from the drop-down list.
4. Click Save.

To delete an agent gateway/Monitor server relationship:

1. In the Mobile Agent Monitor window, select the agent gateway/Monitor server pair you want to delete. You can select more than one row at a time.
2. Click Remove. The selected row is deleted from the table.
3. Click Save.

VoIP Devices

The VoIP Devices window (Figure 24) enables you to enable devices in Unified CM clusters for server-based recording, and to view those already enabled.

Figure 24. VoIP Devices window

The screenshot shows the 'VoIP Devices' window with a search bar at the top. The search criteria are set to 'All Types' in cluster '10.192.252.74' where 'Device Name' matches '*'. Below the search bar is a table with the following data:

Device Name	Device Type	Cluster	Extension	Agent	Monitor Server	Recording Server
SEP00055EE5D08B	Phone	10.192.252.74	1551	dasika, sowjanya...	SPANLINK-SVDGLU	SPANLINK-SVDGLU
SEP0006409CC2F	Phone	10.192.252.74	2301	bauer, andy (bau...	SPANLINK-SVDGLU	SPANLINK-SVDGLU
SEP000967F75761	Phone	10.192.252.74	2456	Almquist, Mike (al...	SPANLINK-SVDGLU	SPANLINK-SVDGLU
SEP0006409EB5B	Phone	10.192.252.74	2341	Knight, Nick (knig...		
SEP0010EB003239	Phone	10.192.252.74	2201	Kaasa, Phil (kaasap)	SPANLINK-43ERG2	SPANLINK-43ERG2

To the right of the table is a 'Bulk Configuration' section with three buttons: 'Configure Monitor Server', 'Configure Recording Server', and 'Remove From Configuration'. At the bottom of the window are buttons for 'Enable Devices for Recording', 'Synchronize Devices With Clusters', 'Save', and 'Cancel'.

NOTE: Extension Mobility is not supported.

The first time this window is accessed, it is empty. You must search the devices configured in Unified CM for the ones you want to enable for server-based recording, and then associate an agent, a QM Monitor service server, and a QM Network Recording service server with those devices.

You can associate the QM Monitor and QM Network Recording service servers with multiple devices at one time. You must associate agents with each device one at a time.

NOTE: You can use the search criteria fields at the top of the window to locate enabled devices. These search criteria fields do not locate

devices that have not yet been enabled. To do that, use the Enable Devices for Recording button.

There are two synchronization issues with the devices listed in this window: synchronizing agents and synchronizing devices.

- An agent configured for a device could be deactivated, lose the agent or knowledge worker role, or become unlicensed. In these cases, the agent will no longer be recorded, and their association with their device is removed. Every time the VoIP Devices window is displayed and the data loaded, the agents are automatically synchronized. You are presented with a list of the invalid agents that will be removed from their associated devices.
- A device could be removed from the Unified CM cluster in which it is configured. You click the Synchronize Devices with Clusters button to view a list of any devices that are configured for server-based recording but that are no longer configured in a cluster. You will be given the option to remove the devices from the VoIP Devices list.

The general procedure for configuring devices for VoIP Monitoring is as follows:

1. Find the devices to be configured.
2. Associate an agent with the device.
3. Associate a QM Monitoring service server with the device.
4. Associate a QM Network Recording service with the device.

To find the devices you want to configure:

1. On the VoIP Devices window, click Enable Devices for Recording. The Search for Devices window appears.
2. Use search criteria fields to locate the devices. You can search by a combination of:
 - Device type (Phone, Remote Agent Port, or All Types)
 - Cluster IP address
 - Device name or extension

You can use wild cards * and ? in the Matches field, as well as specific strings.

By default, the search criteria are set up to return every device in a selected cluster when you click Find.

3. In the list of search results, select the Enabled check box next to the desired devices, and then click OK.

NOTE: You can select multiple rows and click Check Selected or Uncheck Selected to enable or clear multiple devices.

NOTE: If a device has 2 extensions associated with it, it will have 2 entries in the search results table. If you select the Enabled check box for one extension, the other extension will also be selected.

To associate an agent with a device:

1. In the VoIP Devices window, click the device's Agent field to display a drop-down list of agents.

NOTE: You can type text in the drop-down field to filter the list of agents to show only agents whose first name, last name, or Windows login begins with the entered text.

2. Select the appropriate agent from the list. If that agent is already associated with a device, you are asked if you want to switch the association to the current device.
 - If you select Yes, the agent will be associated with this device and removed from the other device.
 - If you select No, no association is made and you can select another agent to associate with this device.
3. Click Save.

To associate a Monitor Server and Recording Server with a device:

1. In the VoIP Devices window, click the device's Monitor Server field to display a drop-down list of servers. Select the appropriate QM Monitor service server from the list.

NOTE: You cannot associate a Monitor Server with a Remote Agent Port (CTI port) device because the QM Monitor service server must be found at run-time.

2. Click the device's Recording Server field to select the appropriate QM Network Recording service server from the drop-down list.
3. Click Save.

To associate multiple devices with a Monitor Server or Recording Server:

1. Select the devices you want to associate with the same Monitor Server or Recording Server.
 - Use Shift + Click to select contiguous rows in the list of devices
 - Use Ctrl + Click to select non-contiguous rows in the list of devices

2. Click Configure Monitor Server or Configure Recording Server, select the appropriate server from the drop-down list, and then click OK. The selected devices are now associated with that server.
3. Click Save.

To remove a device from server-based monitoring:

1. In the VoIP Devices window, select the device you want to delete.
2. Click Remove from Configuration.
3. Click Save.

Introduction

The Personnel node is used to:

- Create groups
- Create knowledge worker teams
- Assign teams to groups
- Assign groups to managers and managers to groups
- Link AD users to ACD users (in Active Directory systems)
- Configure ACD users (in non-Active Directory systems)
- Create QM users
- Assign manager, evaluator, and archive user roles to ACD users
- Assign knowledge worker, supervisor, manager, evaluator, and archive user roles to QM users

User Roles and Privileges

The following is a description of the privileges assigned to each user role.

Agents and Knowledge Workers

Agents and knowledge workers have the following privileges:

- View dashboard with their quality scores and aggregations of their team and group levels
- Export recordings within their scope, if enabled
- Review evaluation results on their own scored contacts
- Enter comments on their own evaluations after the evaluation has been scored
- View their own historical reports

Supervisors

Supervisors have the following privileges:

- View dashboard with their team's and group's quality scores and details of individual agents within their team
- Review evaluation results on all of their team's scored contacts
- Enter comments on their team's evaluations
- Export recordings within their scope, if enabled
- Approve evaluations, if required
- Designate contacts to be retained as Training or HR contacts
- View agent and team-level historical reports
- Evaluate contacts for their team, if enabled to do so
- Access archive recordings for their team

Managers

Managers have the following privileges:

- View dashboard with their group's quality scores and details of individual teams within their group
- Review evaluation results on all of their group's scored contacts
- Enter comments on their group's evaluations
- Approve evaluations, if required

- Export recordings within their scope, if enabled
- Designate contacts to be retained as Training or HR contacts
- View agent, team, group, and enterprise-level historical reports
- Evaluate contacts for their group, if enabled to do so
- Access archive recordings for their group

Archive Users

Archive users have the following privileges:

- Search, review, and export archive recordings for hte enterprise

Evaluators

Evaluators have the following privileges:

- Select, review, and evaluate quality recordings
- Review and add comments to recordings
- Approve evaluations, if required
- Export recordings within their scope, if enabled
- Update previously-scored evaluations

User Administration

The User Administration window displays one of two versions, depending on whether or not your system is configured to interface with Microsoft Active Directory.

Active Directory Systems

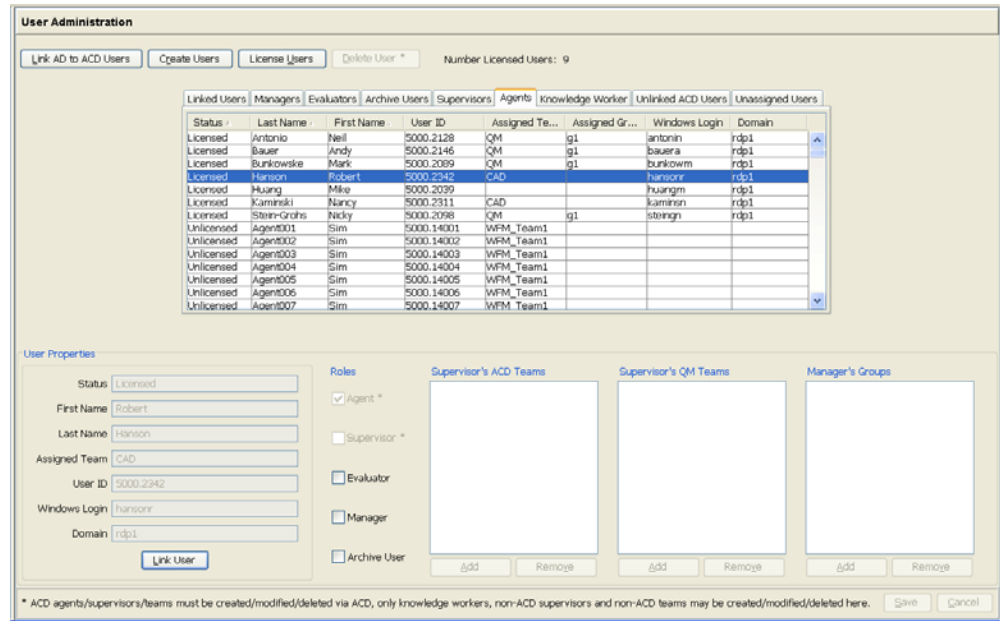
In an Active Directory system, there are three types of users:

- **AD User.** A user set up in Microsoft Active Directory. All users in QM must be in Active Directory. All users in Active Directory must have a first and last name in order to be configured in QM.
- **ACD User.** A user set up as an agent and/or supervisor and assigned to a team in Unified CCX. Manager, evaluator, and archive user roles can be assigned to ACD users in QM.
- **QM User.** A non-ACD user set up in QM.

NOTE: Whenever you make changes to users in Unified CCX—assign them new roles or teams, for example—those changes do not go into effect for the users until the Unified CCX and QM databases are synchronized. You can wait for the automatic synchronization to take place or manually synchronize the databases. See "[Synchronizing Databases](#)" on page 11 for more information.

The User Administration window (Figure 25) has tabs that sort users into categories according to their roles and status within QM.

Figure 25. User Administration window (AD system)



The tabs are described in Table 11.

Table 11. User Administration tabs

Tab	Description
Linked Users	AD users who are linked to an ACD or QM user.
Managers	ACD and QM users assigned the manager role in QM.
Evaluators	ACD and QM users assigned the evaluator role in QM.
Archive Users	ACD and QM users assigned the archive user role in QM.
Supervisors	ACD users assigned the supervisor role in Unified CCX, and QM users assigned the supervisor role in QM.
Agents	ACD users assigned the agent role in Unified CCX.
Knowledge Worker	QM users assigned the knowledge worker role in QM.
Unlinked ACD Users	ACD users who have not been linked to an AD user.
Unassigned Users	QM users who have been created but have not yet been assigned the manager, evaluator, knowledge worker, supervisor, or archive user roles.

Each tab displays information about the users that fall into its category, as shown in [Table 12](#).

Table 12. User Administration tab columns

Column	Description
Status	Licensed or Unlicensed. A user must be licensed in order to be able to log into QM Desktop and to be recorded.
Last Name	The user's last name, as set up in AD.
First Name	The user's first name, as set up in AD.
User ID	The user ID assigned to the user. If the user is an ACD user, the format is <Unified CCX ID>.<CRSresourceID>. If the user is a QM user, it is a number assigned by the QM system.
Assigned Team	The team to which an agent is assigned.
Assigned Group	The group to which an agent is assigned.
Windows Login	The user's Windows user name.
Domain	The domain to which the AD user is assigned.

When you select a user listed in any of the tabs, that user's properties are displayed in the lower section of the window.

Linking ACD Users to AD Users

An ACD user must be linked to an AD user within QM in order to be part of the QM system in some role. An ACD user is assigned the agent role and/or supervisor role in Unified CCX.

You can also assign manager, evaluator, and archive user roles to an ACD user in QM.

NOTE: Unified CCX users might not appear in QM until the Unified CCX and QM databases are synchronized. This process runs automatically at 10-minute intervals. The databases can be manually synchronized if necessary (see "[Synchronizing Databases](#)" on [page 11](#)).

Bulk Linking

When initially setting up QM, you might want to perform a mass linking of ACD to AD users.

To perform bulk linking:

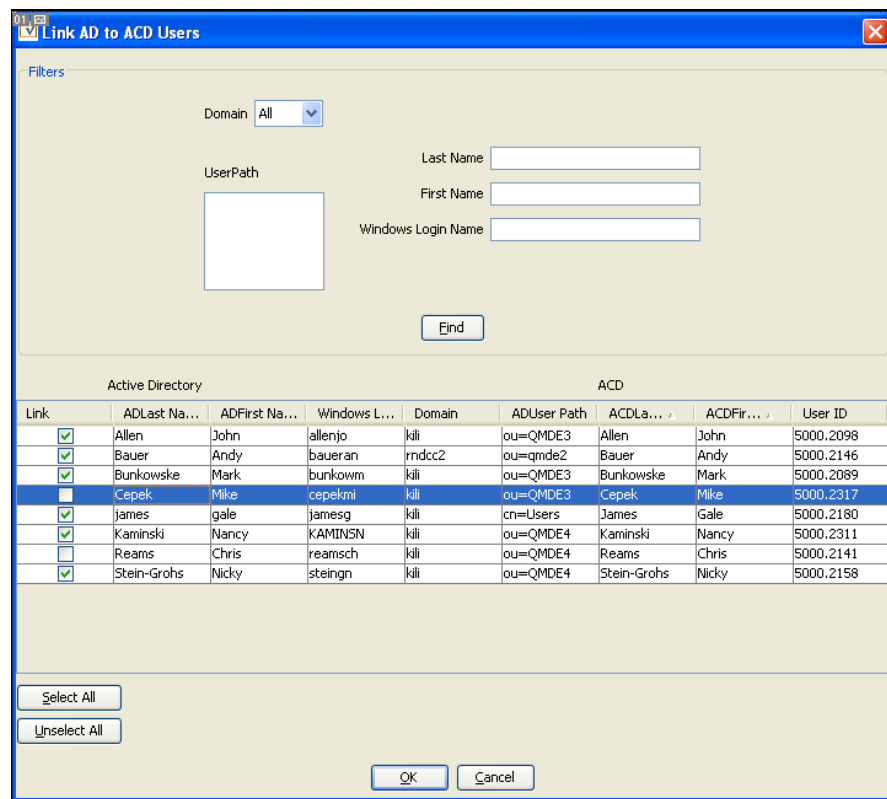
1. In the User Administration window, click Link AD to ACD Users.

The Link AD to ACD Users dialog box appears. AD users whose first and last names match ACD users exactly (ignoring case) are listed (Figure 26).

2. Click Select All to select all entries in the list. If some of the entries should not be linked, you can go through the list and individually clear those check boxes.
3. Click OK.

The AD users and ACD users whose names match exactly are now linked.

Figure 26. Bulk linking AD to ACD users

**Individual Linking****To link an ACD user to an AD user:**

1. On the Unlinked ACD Users tab, select the user you want to link to an AD user.
2. Click Link/Edit Selected User.

The Link Selected User dialog box appears (Figure 27). QM automatically searches on the first two letters of the selected user's first and last name and an asterisk wild card to generate a list of possible matches in AD. You can further narrow the search by specifying the domain and user path, Windows login name, or increasing the number of characters in the first or last name fields, and then clicking Find.

Figure 27. Link Selected User dialog box

Last N...	First N...	Windows ...	Domain	User Path
Reams	Chris	reamsch	kili	ou=qmde4
Reams	Chris	reamsch	rndcc2	ou=qmde1
Repinski	Christina	repinsch	kili	ou=qmde4
Repinski	Christy	repinsc	kili	ou=qmde3

3. Select the AD user name you want to link your ACD user with from the search results, and then click OK.
4. Click Save. The ACD user is now linked to an AD user.

To assign manager, evaluator, and archive user roles to an ACD user:

1. Select the ACD user from one of the tabs in the User Administration window. The user's properties appear in the User Properties section of the window.
2. Select the desired role check box in the Roles section.

If you assigned the Manager role, you can now assign a group to the manager by clicking Add under the Manager's Groups pane and selecting the appropriate group.

3. Click Save.

Switching AD-ACD Links

Once linked to an AD user, an ACD user cannot be unlinked. You can switch a link from one AD user to another AD user by following the procedure for linking an ACD user to an AD user and selecting a new AD user to link to.

If that AD user is already linked to an ACD user, the links will be switched. For example, if:

ACD User 1 is linked to AD User 1
ACD User 2 is linked to AD User 2

and you want to link ACD User 1 to AD User 2, you can do so. The end result is that the links will be switched:

ACD User 1 is linked to AD User 2
ACD User 2 is linked to AD User 1

There are other linking/unlinking situations that can exist. When you attempt to link or unlink various combinations of ACD, AD, and QM users, popup messages appear telling you what you must do to accomplish the task, or if it is allowed in QM.

Deleting an ACD User

You cannot delete an ACD user. However, you can unlicense an ACD user, which means that the user will not be able to log in to QM Desktop and will not be recorded.

For information on unlicensing an ACD user, see "[Licensing Users](#)" on page 73.

Creating a QM User

QM users are users that exist only in QM and AD, and not in Unified CCX. Like ACD users, they must be linked to an AD user in order to be part of the QM system.

A QM user cannot be assigned the agent role, since that is done only in Unified CCX, and QM users do not exist in Unified CCX. QM users can be assigned the knowledge worker, supervisor, manager, evaluator, and archive user roles.

To create a QM user:

1. In the User Administration window, click Create Users.
The Link New Users dialog box appears ([Figure 28](#))

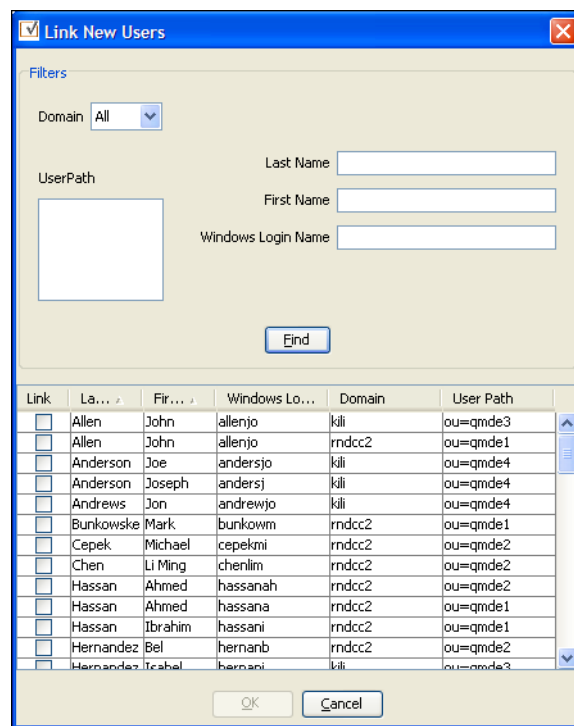
2. Click Find to display a list of all AD users, or enter search criteria to narrow your search results. You can select multiple entries in the list displayed to create more than one QM user at one time.
3. Select the AD user name from the search results you want to link to your new QM user, and then click OK.

The information from the AD user record appears in the User Properties section of the window.

4. Click Save.

The QM user has been created and is linked to an AD user.

Figure 28. Link New Users dialog box



To assign supervisor, knowledge worker, manager, evaluator, and archive user roles to a QM user:

1. Select the QM user from the Unassigned Users tab.

The user's properties appear in the User Properties section of the window.

2. Select the desired role check box in the Roles section.

If you assigned the Knowledge Worker role, you can now assign the knowledge worker to a team using the enabled Assigned Team field. Select the appropriate team from the drop-down list. The team can consist only of knowledge workers.

If you assigned the Manager role, you can now assign a group to the manager. Click Add under the Manager's Groups pane and select the appropriate group.

If you assigned the Supervisor role, you can now assign a team to the supervisor. Click Add under the Supervisor's ACD Teams and/or Supervisor's QM Teams panes and select the appropriate team(s).

3. Click Save.

To delete a QM user:

1. Select the QM user you want to delete on one of the tabs in the User Administration window.
2. Disable all roles the QM user is assigned, remove any team and group associations, and then click Save.
3. Click Delete User. You are asked to confirm that you want to delete the selected QM user.
4. Click Yes. The QM user is deleted.

Non-Active Directory Systems

In a non-Active Directory system, there are two types of users:

- **ACD User.** A user set up as an agent and/or supervisor and assigned to a team in Unified CCX. Manager, evaluator, and archive user roles can be assigned to ACD users in QM.
- **QM User.** A non-agent user set up in QM.

NOTE: Whenever you make changes to users—assign them new roles or teams, for example—those changes do not go into effect for the users until the Unified CCX and QM databases are synced. You can wait for the automatic sync to go through, or manually sync the databases. See "[Synchronizing Databases](#)" on [page 11](#) for more information.

The User Administration window ([Figure 29](#)) has tabs that sort users into categories according to their roles and status within QM. The tabs are described in [Table 13](#).

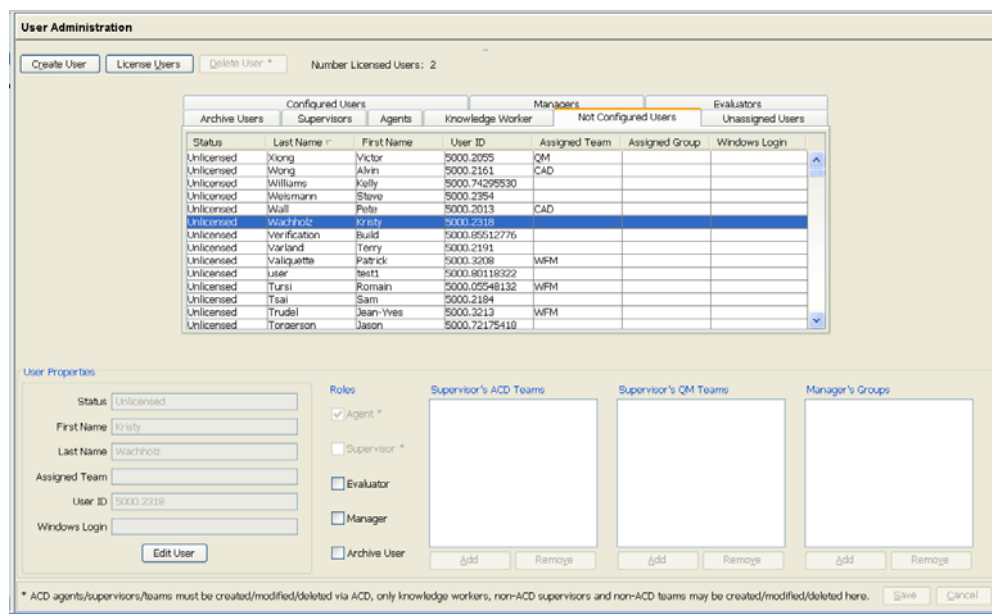
Table 13. User Administration tabs

Tab	Description
Configured Users	All ACD and QM users who have been set up in QM
Managers	ACD and QM users assigned the manager roll in QM
Evaluators	ACD and QM users assigned the evaluator role in QM

Table 13. User Administration tabs (cont'd)

Tab	Description
Archive Users	ACD and QM users assigned the archive user role in QM
Supervisors	ACD users assigned the supervisor role in Unified CCX, or QM users assigned the supervisor role in QM.
Agents	ACD users assigned the agent role in Unified CCX
Knowledge Worker	QM users assigned the knowledge worker role in QM.
Not Configured Users	ACD users who have not yet been set up in QM
Unassigned Users	QM users who have been created but not yet assigned a role in QM

Figure 29. User Administration window (non-AD systems)



Each tab displays information about the users that fall into its category, as shown in [Table 14](#).

Table 14. User Administration tab columns

Column	Description
Status	Licensed or Unlicensed. A user must be licensed in order to be able to log into QM Desktop and to be recorded
Last Name	The user's last name as set up in ACD or QM

Table 14. User Administration tab columns (cont'd)

Column	Description
First Name	The user's first name as set up in ACD or QM
User ID	The user ID assigned to the user. If the user is an ACD user, the format is <Unified CCX ID>.<CRSresourceID>. If the user is a QM user, it is a number assigned by the QM system
Assigned Team	The team to which the user is assigned.
Assigned Group	The group to which the user is assigned.
Windows Login	The user's Windows user name

When you select a user listed in any of the tabs, that user's properties are displayed in the lower section of the window.

Configuring an ACD User

An ACD user must be configured within QM in order to be part of the QM system in some role. An ACD user is always assigned the agent role in Unified CCX, and might also be designated as a supervisor in Unified CCE. Team assignments are also done only in Unified CCX.

The minimum you must do to configure an ACD user in QM is enter the user's Windows login name and QM login password.

NOTE: ACD users may not appear in QM until the Unified CCX and QM databases are synchronized. This process runs automatically at 10 minute intervals. The databases can be manually synchronized if needed (see ["Synchronizing Databases" on page 11](#)).

To configure an ACD user:

1. On the Not Configured Users tab, locate and select the user you want to configure.
2. In the Properties section, enter the user's Windows Login Name and QM Login Password.

NOTE: The Windows login name must be unique, but users can have the same first and last names. It must be between 1 and 64 characters long, cannot consist entirely of spaces, and cannot include these characters: / \ [] ; " | = , + * ? < > ()

3. If necessary, assign the user the Evaluator, Archive User, and/or Manager role by selecting the check boxes next to those roles.

If you assigned the Manager role, you can now assign a group to the manager by clicking Add under the Manager's Groups pane and selecting the appropriate group.

4. Click Save.

The ACD user is now moved from the Not Configured User tab and is listed under the tab for each role you assigned to the user. For instance, if the ACD user was assigned the role of evaluator, he or she is listed under both the Agents tab and the Evaluators tab.

NOTE: Because ACD users are always agents and/or supervisors, they are never listed on the Unassigned Users tab. They are listed on the Agents and/or Supervisors tabs. QM users are never agents, and so can be listed on the Unassigned Users tab.

Unconfiguring or Deleting an ACD User

Once configured in QM, an ACD user cannot be unconfigured or deleted. However, you can unlicense an ACD user, which means that the user will not be able to log in to QM Desktop and will not be recorded.

For information on unlicensing an ACD user, see ["Licensing Users" on page 73](#).

Creating a QM User

A QM user is a user created in QM that does not exist in Unified CCX. A QM user can be an evaluator, manager, supervisor, knowledge worker, and/or archive user, but not an agent.

To create a QM user:

1. Click Create User.

The User Properties section becomes enabled.

2. Complete the First Name, Last Name, Windows Login Name, and QM Login Password fields. You can assign a role to the new user at this time, or do it later.

NOTE: The Windows login name must be unique, but users can have the same first and last names.

3. Click Save.

The new QM user is assigned a QM User ID and is now listed on the tab for each role you assigned the user, or on the Unassigned Users tab if you have not assigned any roles.

Assigning Roles to a QM User

You can assign the Supervisor, Knowledge Worker, Evaluator, Archive User, and Manager roles to a QM user from any tab on which that user is listed.

To assign supervisor, knowledge worker, manager, evaluator, and archive user roles to a QM user:

1. Select the QM user from any tab on which the user is listed.

The user's properties appear in the User Properties section of the window.

2. Select the desired role check box in the Roles section.

If you assigned the Knowledge Worker role, you can now assign the knowledge worker to a team using the enabled Assigned Team field. Select the appropriate team from the drop-down list. The team can consist only of knowledge workers.

If you assigned the Manager role, you can now assign a group to the manager by clicking Add under the Manager's Groups pane and selecting the appropriate group.

If you assigned the Supervisor role, you can now assign the supervisor using the enabled Assigned Team field. Select the appropriate team from the drop-down list. The selected team can be either an ACD or non-ACD team.

NOTE: You must first assign the QM user the knowledge worker role before you can assign that user the Supervisor role.

3. Click Save.

Licensing Users

Users must be licensed in order to log into QM Desktop and to be recorded. A user's license status is displayed in the User Administration window.

The total number of licensed users is displayed on the User Administration interface to the right of the License Users button. The number displayed updates as soon as you license/unlicense users.

Users' license status can be changed only after they have been linked to an AD user (in AD systems) or configured (in non-AD systems).

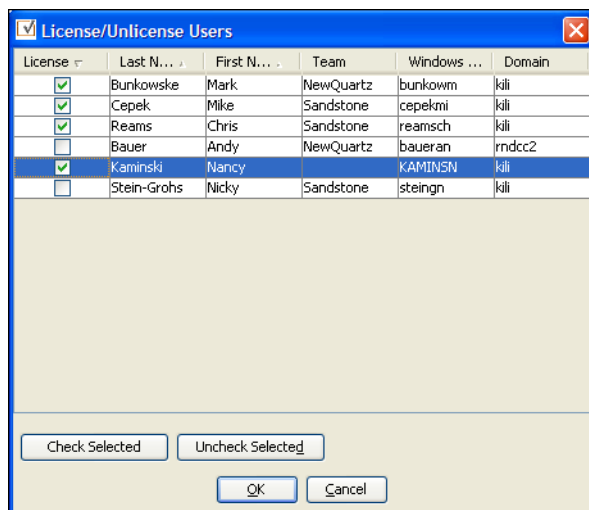
The number of licenses you have is configured when your system is installed. More information about managing your licenses can be found in "[Licenses](#)" on page 27.

To change a user's license status:

1. Click the License Users button.

The License/Unlicense Users dialog box appears (Figure 30). It displays a list of all linked users.

Figure 30. License/Unlicense Users dialog box



2. Select or clear the License check box next to the linked user(s) whose license status you want to change, and then click OK.

You can select or clear multiple check boxes by holding the Shift key while selecting contiguous users, or by holding Ctrl while selecting non-contiguous users, and then clicking either the Check Selected or Uncheck Selected buttons.

The users whose status is now Licensed can now log into QM Desktop and be recorded.

Team Administration

The Team Administration window (Figure 31) enables you to:

- View the agents and supervisors belonging to a selected team
- Assign QM supervisors to a team of ACD agents
- Create, rename, and remove QM teams
- Assign to QM users, ACD supervisors, and QM supervisors to QM teams

Figure 31. Team Administration window

The screenshot shows the 'Team Administration' window with the following components:

- Team Selection:** A dropdown menu showing 'Team QM' and buttons for 'New', 'Delete', and 'Rename'.
- Assigned Agents Table:**

Last	First	ID
Allen	John	5000.2158
Antonio	Neil	5000.2128
Bauer	Andy	5000.2146
Bunkowske	Mark	5000.2089
Ceppek	Mike	5000.2317
Kaasa	Phil	5000.2011
Shako	Nicholas	5000.2109
Stein-Grohs	Nicky	5000.2098
Xiong	Victor	5000.2055
- Assigned ACD Supervisors Table:**

Last	First	ID
Kaasa	Phil	5000.2011
Stein-Grohs	Nicky	5000.2098
test11	qa	5000.86080626
test12	qa	5000.66200472
- Assigned QM Supervisors Table:**

Last	First	ID
Bose	Tom	0.5
Jones	Andrea	0.2
- Buttons:** 'Add' and 'Remove' buttons are located below each table. At the bottom right, there are 'Save' and 'Cancel' buttons.

Agents and ACD supervisors are assigned to teams in Unified CCX, and therefore cannot be changed from within QM. You can assign QM supervisors to an ACD team.

QM users cannot be assigned to the same team as ACD users. They must belong to a team made up only of QM users. However, a QM team can have ACD supervisors as well as QM supervisors.

You cannot create, rename or remove an ACD team. Those teams are created in Unified CCX.

To assign a QM supervisor to a team:

1. Under the Assigned QM Supervisors pane, click Add.
The Select QM Supervisors dialog box appears.
2. Select the supervisor you want to assign to the team, and then click OK.

To remove a QM supervisor from a team:

- Select the QM supervisor you want to remove from the team from the Assigned QM Supervisors pane, and then click Remove.

To create a QM team:

1. Click New next to the Team field.
The Create New Team dialog box appears.
2. Type the name of the new QM team, and then click OK.
3. Add knowledge workers, ACD supervisors, and QM supervisors to the new team by clicking Add underneath each pane, selecting the desired names from the list, and then clicking OK.
4. When the new QM team is complete, click Save.

To rename or delete a QM team:

1. Select the team from the Team field, and then do one of the following.
 - To rename the team, click Rename, type the new name in the Rename Team dialog box, and then click OK.
 - To delete the team, click Delete. You will be asked to confirm the deletion. Any knowledge workers assigned to that team will no longer be recorded when the team is deleted.

Group Administration

Groups are made up of teams and have managers assigned to them. Using QM Administrator, you can:

- Create, rename, and delete a group
- Add and remove teams from a group
- Add and remove managers from a group

Adding a New Group

You can add as many groups as desired to QM.

NOTE: Each group's name must be unique.

To create a new group:

1. In the navigation tree, select Personnel > Group Administration.

The Group Administration window appears ([Figure 32](#)).

Figure 32. Group Administration window

The screenshot shows the 'Group Administration' window. At the top, there is a 'Group' dropdown menu set to 'Midwest', and three buttons: 'New', 'Delete', and 'Rename'. Below this, there are two main sections: 'Assigned Teams' and 'Assigned Managers'. The 'Assigned Teams' section contains a list box with 'Larch', 'Oak', and 'Silver' and 'Add' and 'Remove' buttons below it. The 'Assigned Managers' section contains a table with columns 'Last', 'First', and 'ID', and 'Add' and 'Remove' buttons below it.

Last	First	ID
Allen	John	5000.2098
Lincoln	Abraham	5000.2071

2. Click New.
The Create New Group dialog box appears.
3. Enter the name of the new group, and then click OK.
The new group is added to the Group drop-down list.

Assigning Teams and Managers to a Group

Once a group is set up you can assign teams and managers to it. A team must be assigned to a group in order for the team’s agents to be recorded as part of a workflow.

To assign teams to a group:

1. Select the group from the Group drop-down list.
The Group Administration window displays any teams already assigned to the group. If there are no teams assigned to the group, the Assigned Teams pane is empty.
2. Click Add under the Assigned Teams pane.
The Select Teams dialog box appears (Figure 33).

Figure 33. Select Team dialog box



3. Select the team or teams you want to assign to the group from the list of available teams. Use Shift + Click to select adjacent teams and Ctrl + Click to select non-adjacent teams.

NOTE: A team can belong to only one group. If you assign a team to a group and it already belongs to another group and is not associated with any workflows, QM will ask you to confirm moving the team from one group to another group.

4. Click OK.

The teams you selected are now listed in the Assigned Teams pane.

5. Click Save.

To add managers to a group:

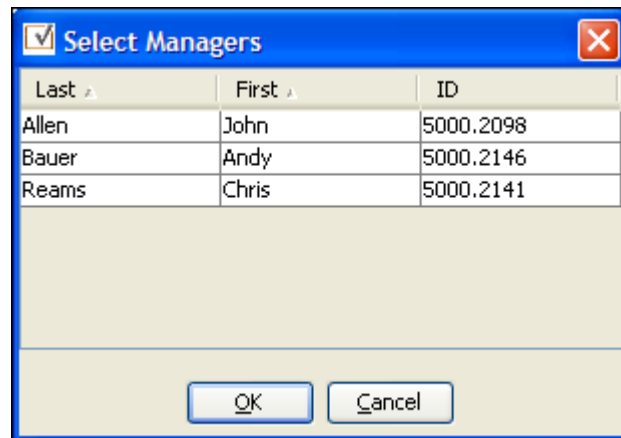
1. Select the group from the Group drop-down list.

The Group Administration window displays any managers already assigned to the group. If there are no managers assigned to the group, the Assigned Managers pane is empty.

2. Click Add under the Assigned Managers pane.

The Select Managers dialog box appears (Figure 34).

Figure 34. Select Managers dialog box



3. Select the manager or managers you want to assign to the group from the list of available managers. Use Shift + Click to select adjacent managers and Ctrl + Click to select non-adjacent managers.

A manager can be assigned to more than one group, and a group can have multiple managers.

4. Click OK.

The managers you selected are now listed in the Assigned Managers pane.

5. Click Save.

Removing Teams and Managers From a Group

To remove a team from a group:

1. In the Group Administration window, select the group the team belongs to from the Group drop-down list.
2. In the Assigned Teams pane, select the teams you want to remove from the group, and then click Remove.
3. Click Save.

The teams are removed from the group and are available to be reassigned to another group.

To remove a manager from a group:

1. In the Group Administration window, select the group the manager is assigned to from the Group drop-down list.
2. In the Assigned Managers pane, select the managers you want to remove from the group, and then click Remove.
3. Click Save.

The managers are removed from the group.

Renaming a Group

To rename a group:

1. In the Group Administration window, select the group you wish to rename from the Group drop-down list, and then click Rename.

The Rename Group dialog box appears.

2. Enter the new name for the group, and then click OK.

The group's new name is shown in the Group drop-down list.

Deleting a Group

You cannot delete a group if any teams in that group are assigned to a workflow. Those teams must be removed from the workflow before the group can be deleted.

To delete a group:

1. In the Groups Administration window, select the group you wish to delete from the Group drop-down list, and then click Delete.
2. You are asked to confirm if you wish to delete that group. Click Yes to delete the group.

Any teams that were assigned to that group appear in the Select teams dialog box (see [Figure 33 on page 78](#)) with no group affiliation, and the group is deleted from the Group drop-down list.

Introduction

The Recordings node enables you to:

- Configure recording retention periods
- Configure archiving at the team level
- Configure and manage user-defined metadata
- Enable/disable recording export at the role level
- Create workflows

About Recordings

There are two types of recordings: those made for quality management purposes, and those made for archiving purposes. Quality management recordings can include screen recordings. Archive recordings are voice only.

When archiving for a team is enabled, all inbound and outbound calls made by that team are recorded and kept for a period set by the QM administrator.

Quality management recordings use workflows to determine which recordings of inbound and/or outbound calls (“calls of interest”) to save for evaluation. Some examples of why you would record calls of interest are:

- Tracking the performance of specific agents
- Helping train new agents
- Monitoring calls during a sale period
- Monitoring calls during specific times of day
- Monitoring calls from specific customers or phone numbers

A recording must be at least 5 seconds long to be displayed in QM. A recording of less than 5 seconds is not considered a valid recording.

The time associated with a contact is the time the contact occurred at the agent's location, expressed in 24-hour HH:MM:SS format. For example, if the agent is located in Chicago, the time associated with any recorded contacts made by that agent is Chicago local time.

The contact also displays the abbreviation for the local time zone. If the time zone associated with the contact is unknown to QM, then the time is displayed in Greenwich Mean Time (GMT).

About User-Defined Metadata

Administrators can add up to 10 use-defined metadata fields. The metadata can be captured from Cisco Unified CCX, Cisco Agent Desktop (CAD), and other applications using a third-party API to pass the data to QM. The CAD IPC Action can also be used to pass data to QM. See the *Cisco Desktop Administrator User Guide* for more information.

Configuring Recording Retention Periods

The length of time that quality management recordings and archive recordings are retained is configured under the Recordings node.

Every day at the time set in the Database Cleanup Time field in the Upload Settings window (see "[Upload Settings](#)" on page 31), the database cleanup utility deletes recordings whose retention period has expired.

NOTE: It is important to remember that reducing a retention period after it has been set initially can result in the deletion of recordings, and that increasing a retention period will result in a larger use of storage space. Changing these values should be considered carefully.

Quality Management Recordings

To configure quality management recording retention periods:

1. In the navigation tree, select the Recordings > Quality Management node. The Quality Management Recordings Administration window appears ([Figure 35](#)).

Figure 35. Quality Management Recordings Administration window



The screenshot shows the "Quality Management Recordings Administration" window. It features a "Recordings Retention" section with the following settings:

- Scored (10 - 60 days): 30
- Unscored (10 - 60 days): 30
- HR (2 - 12 months): 6
- Unlimited
- Training (2 months - unlimited): 6
- Unlimited
- Agent Tagged (12 months - unlimited): 120

At the bottom right, there are "Save" and "Cancel" buttons.

2. Set the length of time you want the various types of recordings to be retained:

- Scored—recordings that have been evaluated and scored
- Unscored—recordings that have yet to be evaluated, are in progress, or are awaiting approval
- HR—recordings that have been evaluated and tagged with the HR tag
- Training—recordings that have been evaluated and tagged with the Training tag
- Agent Tagged—recordings that have been tagged by an agent for retention

If you want Training or Agent Tagged recordings to be retained indefinitely, select the Unlimited check box.

3. Click Save.

Archive Recordings

To configure archive recording retention periods:

1. In the navigation tree, select the Recordings > Archive node. The Archive Recordings Administration window appears (Figure 36).

Figure 36. Archive Recordings Administration window

2. Use the arrow buttons to move teams to the Non-Archive Teams or Archive Teams panes as desired. By default all teams are in the Non-Archive Teams pane.
3. In the Archive Upload Time field, set the time when recordings are uploaded from client computers to the archive location.

NOTE: If a team has a quality management recording workflow set up in addition to site archiving, the End of Day time that is configured on the Workflow Administration window (Figure 41 on page 96) will be used instead of the time set in the Archive Upload Time field, and all

recordings, including those recorded for archiving, will be uploaded at that time.

4. Enter the number of months the recordings are to be archived. The minimum number of months recordings can be archived is 12 (1 year).

If you want the archived recordings to be retained indefinitely, select the Unlimited check box.

5. Click Save.

Enabling Recording Export

Contact recordings are stored in a format that is not playable by non-QM playback software. However, recordings can be exported in the following formats, which are playable in other playback software (such as Windows Media Player):

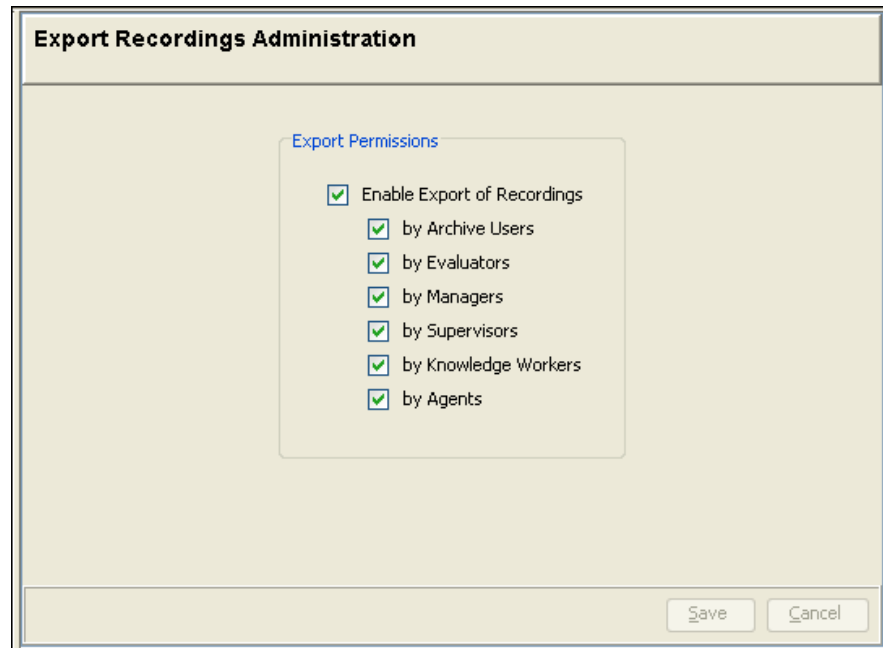
- WAV format (uncompressed audio)
- WMA (compressed audio)
- WMV (compressed audio/video)

By default, the export feature is disabled.

To enable recording exports:

1. In the navigation tree, select the Recordings > Export node. The Export Recordings Administration window appears (Figure 37).

Figure 37. Export Recordings Administration window



2. Select the check boxes next to the roles you want to be able to export recordings. If you select the Enable Export of Recordings check box, all roles are selected. If you clear the Enable Export of Recordings check box, all roles are cleared.
3. Click Save.

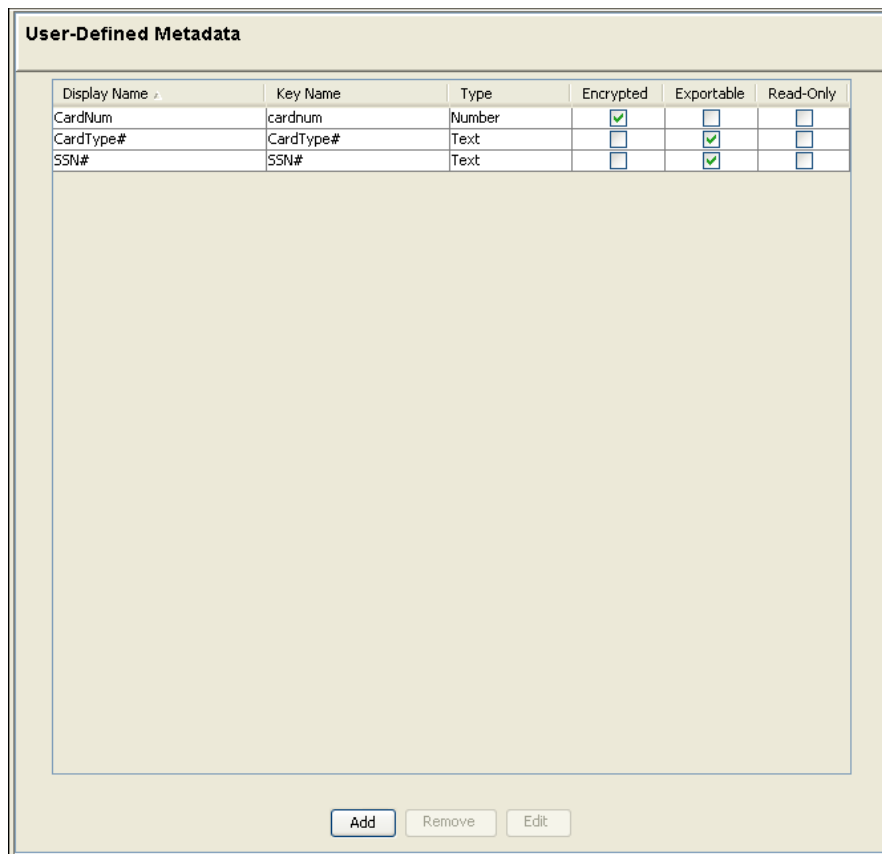
Configuring User-Defined Metadata

User-defined metadata is configured and managed under the Recordings node.

To add a user-defined metadata field:

1. In the navigation tree, select the Recordings > Metadata node. The User-Defined Metadata window appears (Figure 38).

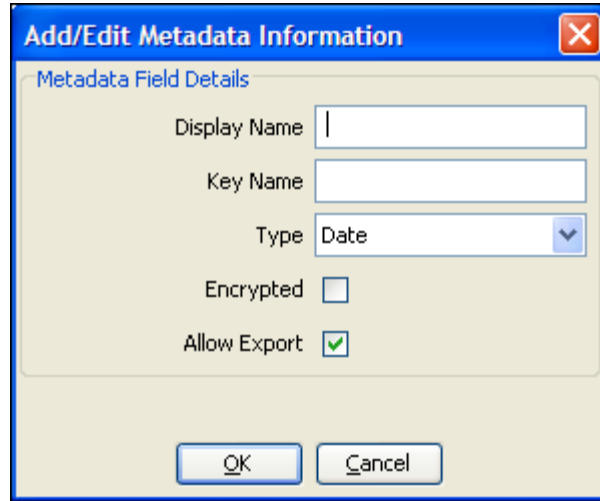
Figure 38. User-Defined Metadata window



NOTE: Metadata is tagged as read-only if it is obtained from Interaction Analytics. This metadata cannot be edited, it can only be viewed.

2. Click Add. The Add/Edit Metadata Information dialog box appears (Figure 39).

Figure 39. Add/Edit Metadata Information dialog box



3. Complete the fields as follows:

Field	Description
Display Name	The metadata field name that is seen in search results tables and contact information. Maximum is 64 characters, not restricted to any type of character.
Key Name	A unique identifier for the metadata field, used by APIs. Maximum is 39 characters. The following characters are not allowed: <ul style="list-style-type: none"> • space • & (ampersand) • = (equal sign)
Type	Select the type of information the field holds: Text, Date, or Number.
Encrypted	Select this check box if you want the metadata to be encrypted when stored.
Allow Export	Select this check box if you want to be able to export the metadata via API or desktop. By default this check box is selected. Metadata that is encrypted cannot be exported.

4. Click OK to create the metadata field.

To edit a metadata field:

1. In the User-Defined Metadata window, select the metadata field you want to edit, and then click Edit. The Add/Edit Metadata Information dialog box appears (Figure 39). Note that in Edit mode, the Key Name and Encrypted fields are disabled and cannot be edited.
2. Make the desired changes to the editable Display Name and Type fields, and then click OK. Your changes appear in the list of metadata fields.

To remove a metadata field:

1. In the User-Defined Metadata window, select the metadata field you want to remove, and then click Remove.

The message, "This will immediately delete all metadata records corresponding to the metadata field <field name>. Continue?" appears.
2. Click Yes to confirm you want to delete the metadata field, or No to cancel the deletion. If you clicked Yes, the field is removed. If you clicked No, the action is canceled.

Creating a Workflow

Before you create a workflow:

- Set up users and groups
- Assign teams to a group. Unassigned teams cannot be added to a workflow
- Create an active evaluation form

When setting up a new workflow, the general procedure is as follows:

1. Name the new workflow and add teams to it
2. Configure the end of day and the number of recordings per day per agent
3. Configure one or more classifiers to set which evaluation form is used and which calls are recorded based on call direction, calling or called numbers, and other filters
4. Configure rules for the Ringing, Answered, and Dropped events for each classifier (only if Classifier With Rules is selected)

NOTE: Unless an agent is part of a workflow, no recordings made of that agent will appear in the QM Desktop Recording tab. If archiving is enabled, they will appear in the Archives tab.

How Multiple Classifiers in a Workflow are Executed

You can set up multiple classifiers for a workflow. They are executed in the order they are listed (from top to bottom) in the workflow navigation tree. This enables you to create classifiers that are subsets of more general classifiers.

To change the order of classifiers in the navigation tree, select the classifier and use the Up and Down arrow buttons to move it up or down in the navigation tree.

Example

Classifier 1:

- Called number = 20??
- Inbound
- Rule 1: record new employee J. Smith
- Rule 2: record random calls for Team A

Classifier 2:

- Calling number = * (all)
- Outbound

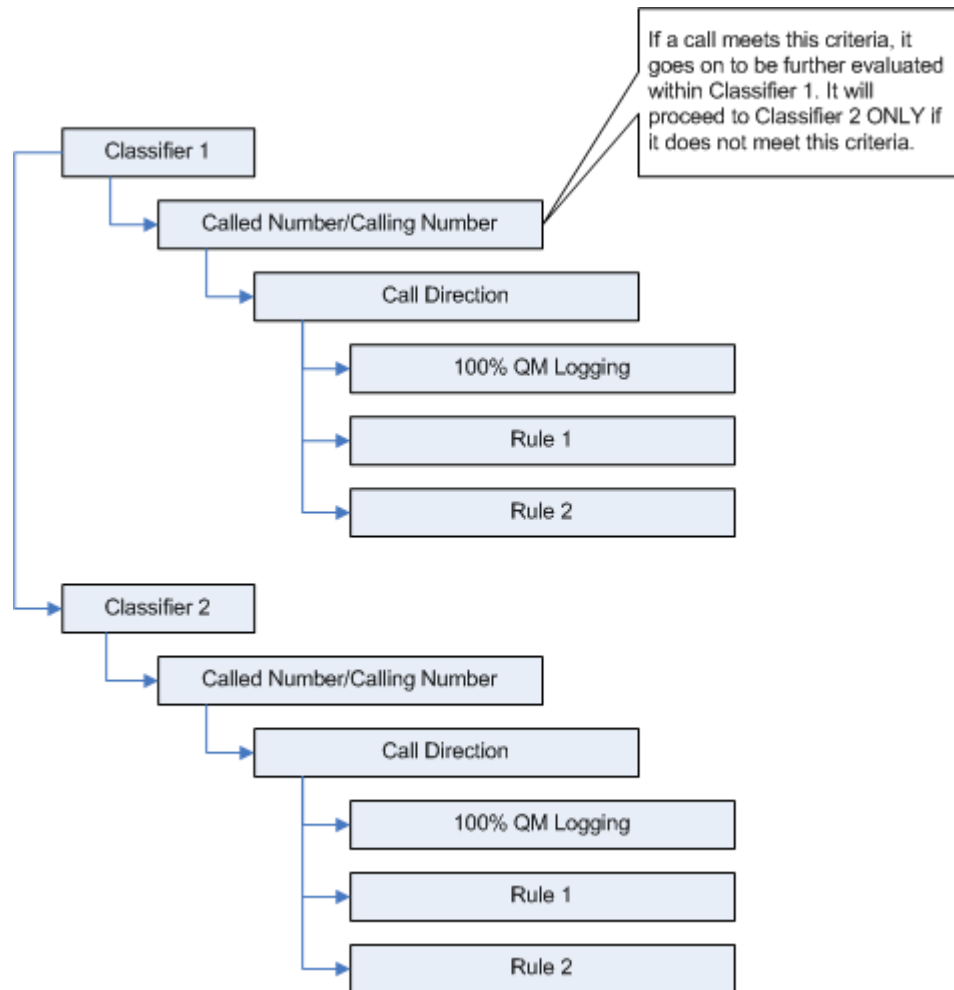
- Rule 1: record longest call of the day (50%) and shortest call of the day (50%) for Team B

In this example, a call must meet the called number criteria and then the call direction criteria of Classifier 1 in order to go on to evaluate the rules. If the call does not meet the called number criteria, the workflow moves on to Classifier 2.

If, however, the call meets the called number criteria and the call direction criteria of Classifier 1, the workflow then goes on to evaluate the rules in top-down order. If none of the rules are met, the call will not be marked for Quality Management (although it might be uploaded for archiving if archiving is enabled).

Once a contact matches a classifier (and does or does not match any of those classifier's rules), it will not move on to another classifier.

Figure 40. Classifier execution order



Creating a New Workflow

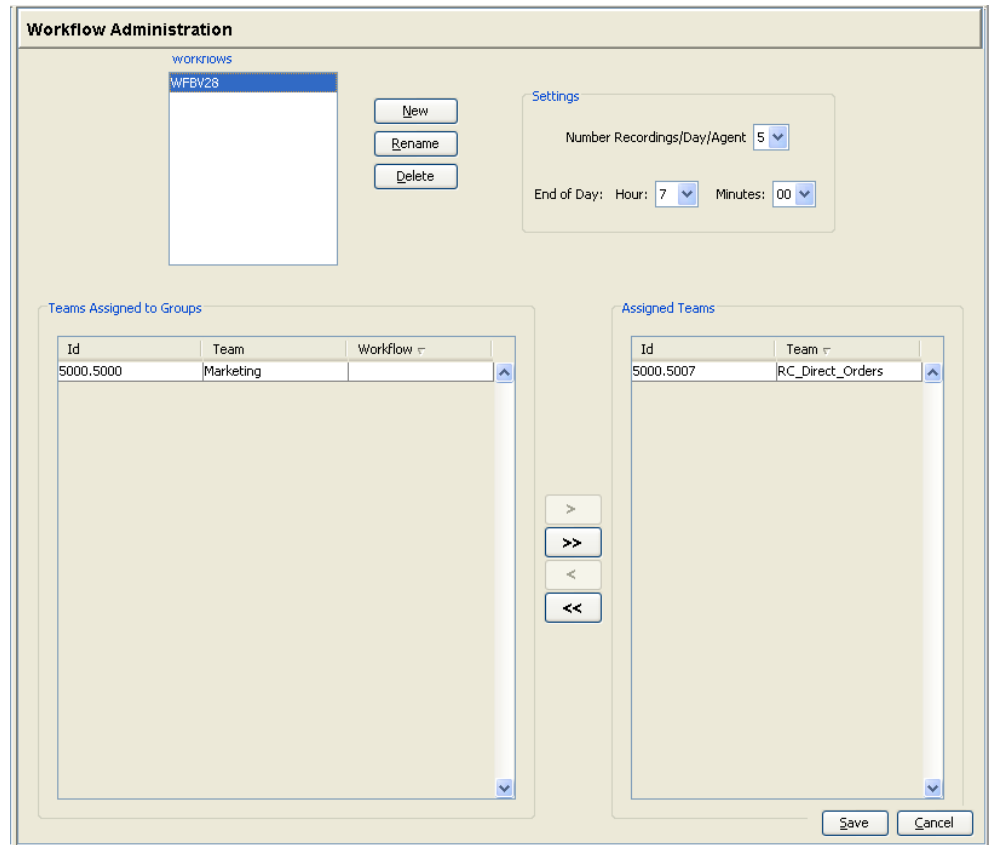
To name the new workflow, configure it, and add teams:

1. In the navigation tree, select Recordings > Quality Management > Workflows.
The Workflow Administration window appears ([Figure 41](#)).
2. Next to the Workflows pane, click New.
The Workflow Name dialog box appears.
3. Enter a name for the new workflow, and then click OK.
The workflow is now listed in the Workflows pane.
4. Select the workflow, and complete the rest of the window.
 - a. In the Settings section, select the number of recordings per day per agent that will be made under this workflow. The maximum number is 5.
 - b. Enter when the end of the work day is, in 24-hour format. The end of day is when the uploading process begins. Recording still continues, but those recordings are uploaded after the next end of day.
 - c. Assign teams to the workflow. A team can belong to only one workflow at a time. If a team you want to assign to this workflow is already assigned to another workflow, it is automatically reassigned to this workflow. A warning message is displayed telling you that the team is being reassigned from another workflow.

NOTE: A team must be assigned to a group in order to be assigned to a workflow. If a team is not assigned to a group, it does not appear in the Workflow Administration window.

- When you are done configuring the workflow in this window, click Save.

Figure 41. Workflow Administration window



Setting Up Classifiers

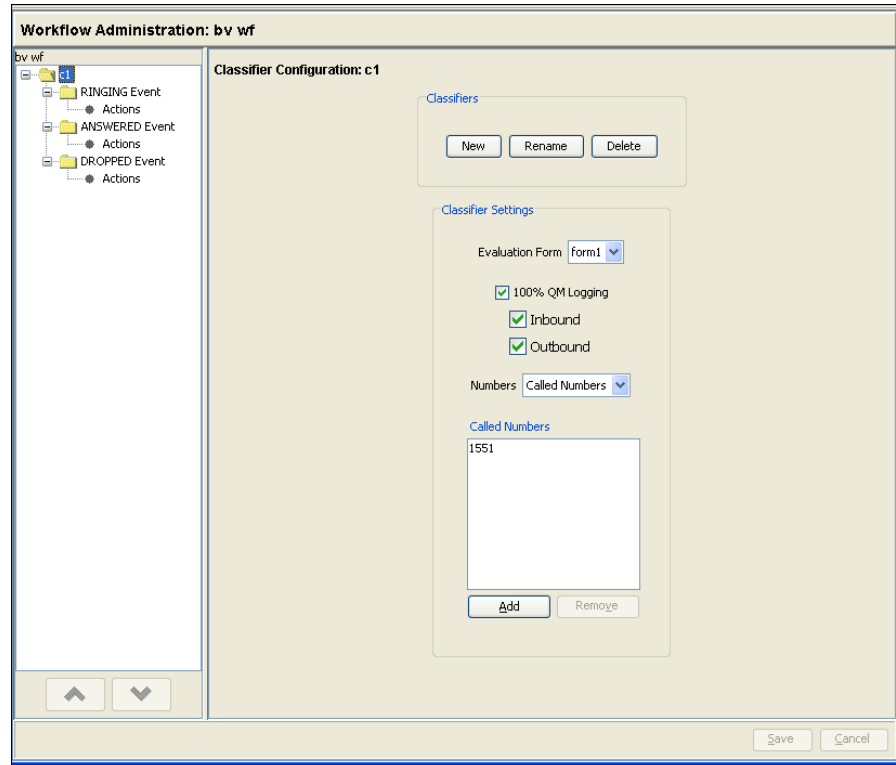
Classifiers are filters that determine which calls are recorded.

To set up classifiers:

- Under the Workflow node, select the workflow you just created.

The <workflow name> Workflow Classifier Configuration window appears (Figure 42).

Figure 42. Workflow Classifier Configuration window



2. In the Classifiers section, click New to create a new classifier.
The Classifier Name dialog box appears.
3. Enter a name for your new classifier, and then click OK.
The new classifier is now listed in the workflow navigation tree.
4. Select the new classifier in the workflow navigation tree.
5. In the Classifier Settings section, complete all fields as follows:

Field/Option	Description
Evaluation Form	Select the form you want to use to evaluate the recorded calls.
100% QM Logging	Select this option if you want to configure a classifier that does not use rules, but rather records all calls defined by the classifier.

Field/Option	Description
Inbound and/or Outbound	Select which calls to be recorded—inbound, outbound, or both. You must select at least one call direction.
Numbers	Select the type of number you want to use to filter the calls to be recorded, Called Number or Calling Number. The Called Number is either the route point number if the call was routed, or the agent extension if it was direct dial. The Calling Number is the original number from which the caller is dialing. Note: If you change your selection here from Calling Number to Called Number or vice versa after entering phone numbers in the Called/Calling Numbers field, all entered numbers will be lost. You will have to define them again.
Called/Calling Numbers	Click Add to specify the phone numbers you want to filter for in the Numbers field. You can enter: <ul style="list-style-type: none"> • Specific numbers (for example, 6125551212) • Number ranges using wild cards (for example, 612*, where the * wild card stands for any number of digits, or 612555????, where the ? wild card stands for 1 digit) • The * wild card to record all calls The numbers you enter cannot contain dashes or parentheses, and must be between 1 and 16 characters long.

6. Click Save to save the classifier settings.

NOTE: If you did not select 100% QM Logging, you must now configure at least one rule. See ["Setting Up Rules" on page 99](#) for more information.

Configuring Actions

Under each event in the workflow navigation tree is an Action node. The action nodes control whether or not a voice recording and/or video recording starts. By default, the action settings are enabled.

All voice and screen recording is stopped immediately at logout, shutdown, or configured end of day.

To configure actions for the Ringing, Answered, and Dropped events:

1. Under Ringing Event, select the Start Screen Recording check box if you want the video recording to start when the phone rings (not available in the Basic feature level).
2. Under Answered Event, select the Start Voice Recording check box if you want the audio recording to start when the phone is answered.
3. Under Dropped Event, select the Stop Voice Recording and/or Stop Screen Recording check boxes if you want the audio and/or video recording to stop when the call is dropped (Stop Screen Recording not available in the Basic feature level).

If you want screen recording to continue during after-call work, enter the amount of time (in seconds) the recording period should go after the call is dropped in the Extend Screen Recording field. Note that if another call starts before the configured time period is over, the recording is automatically stopped so that recording the new call can start.

4. Click Save to save the action settings.

Setting Up Rules

You must set up at least one rule if you have configured the classifier without 100% QM Logging. Rules do not apply to classifiers that are configured with 100% QM Logging.

To set up rules to apply to the classifier's Ringing event:

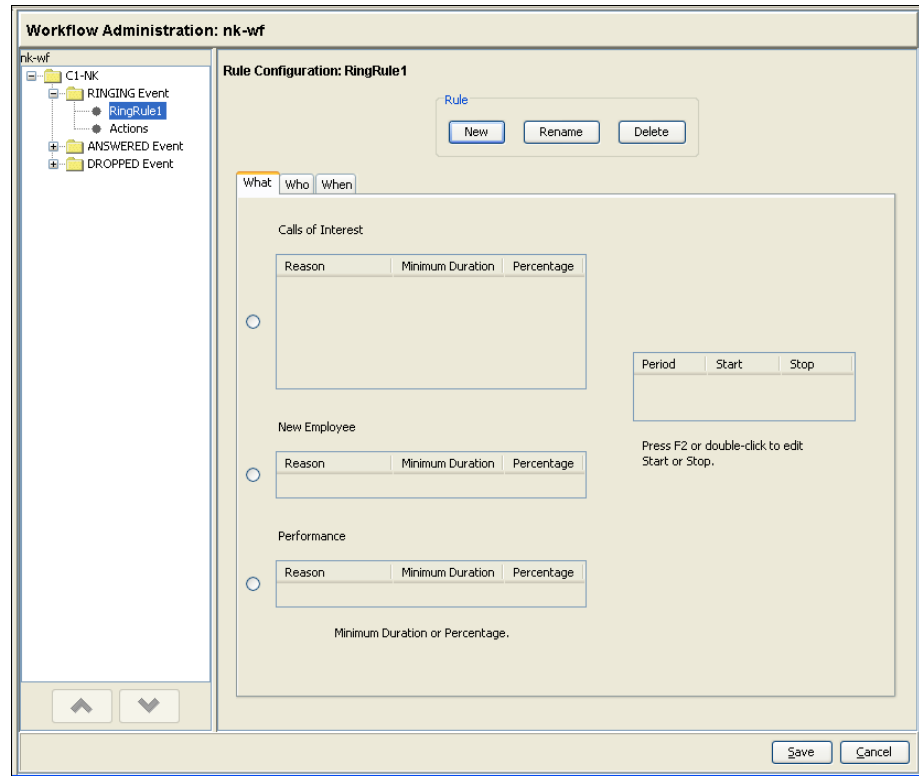
1. In the workflow navigation tree, under the classifier, select the Ringing event.
The Rule window appears.
2. Click New to add a new rule.
The Rule Name dialog box appears.
3. Enter a name for the new rule, and then click OK.
The new rule is now added to the workflow navigation tree underneath the Ringing event.

NOTE: As with classifiers, multiple rules may be set up and ordered from most to least specific.

4. In the workflow navigation tree, select the rule.
The Rule setup window appears.

5. On the What tab (Figure 43), select the calls that will be recorded.

Figure 43. Rule Setup window—What tab



There are three categories of calls:

- **Calls of Interest.** Select this category when you want to record a type of call. They are:
 - First Call of Day
 - Last Call of Day
 - Longest Call of Day
 - Shortest Call of Day
 - Random Call (random calls during a specified time period)

Enter a minimum call duration and percentage of total calls recorded for the specific type of call you want to record. The shortest minimum duration allowed is 5 seconds. For Random calls you must also set up one or two periods with a start and stop time. To enter or modify the minimum call duration, double-click the Minimum Duration field, or click the field and press F2, and then enter the desired call duration. To modify the percentage field, click the field and select the desired percentage from the drop-down list.

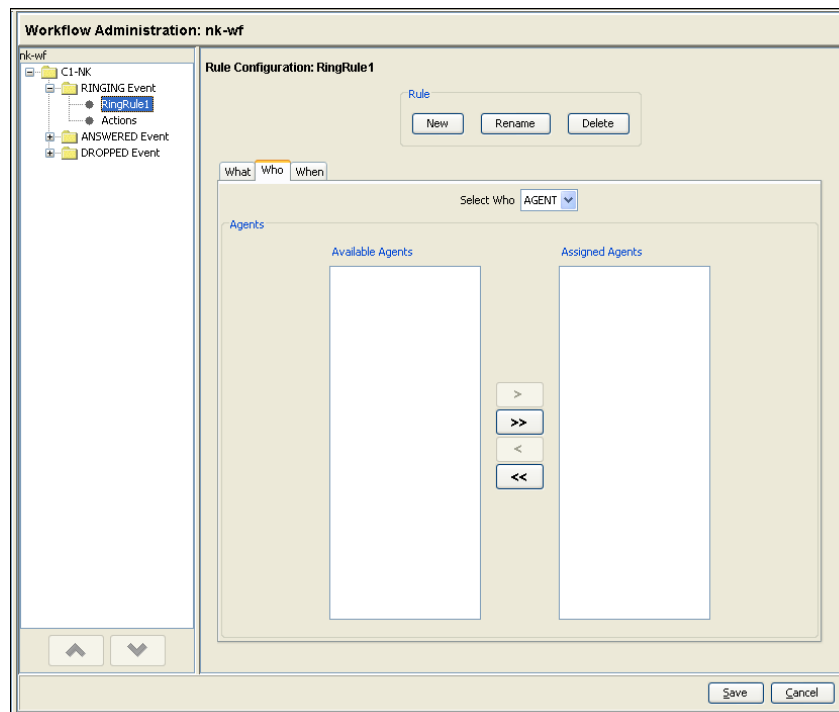
- **New Employee.** Select this category if you want to record all of a new agent’s calls. Enter a minimum call duration. The percentage of calls recorded and uploaded is automatically set to 100%. You must also select the specific employee on the Who tab and a date range on the When tab (up to a maximum of 10 days).
- **Performance.** Select this category if you want to monitor an agent’s performance. Enter a minimum call duration. The percentage of calls is recorded and uploaded is automatically set to 100%. You must also select the specific employee on the Who tab and a date range on the When tab (up to a maximum of 10 days).

The values that appear in the Calls of Interest table’s Percentages field depends on the number of total recordings per day per agent you configure in the Workflow Administration window. For example, if you set the number at 5 recordings, the values that appear in the Percentages drop-down list are 0, 20, 40, 60, 80, and 100. If you set the number at 3, the values that appear are 0, 33, 67, and 100.

The sum of the percentages you select in the Calls of Interest table does not have to equal 100%. If the sum is 80%, then four-fifths of the recordings are saved for this rule.

6. On the Who tab (Figure 44), from the Select Who drop-down list, select either Agent or Team.

Figure 44. Rule Setup window—Who tab



7. In the Available Agents/Available Teams pane, select the agent or team you want the workflow to apply to, and use the arrow buttons to move those agents or teams to the Assigned pane.

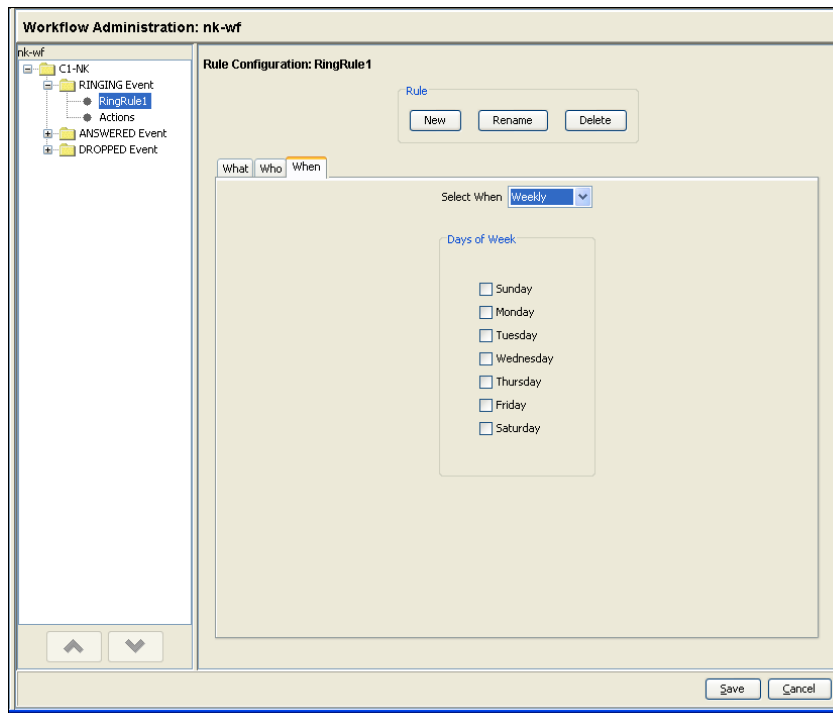
You can only select one agent if you selected New Employee or Performance on the What tab.

8. On the When tab (Figure 45), select when the workflow will run from the When drop-down list:
 - Set of Dates—select specific dates.

NOTE: The Set of Dates setting is required for Performance and New Employee recordings, with a maximum of 10 days.

- Weekly—select the days of the week
- Date Range—select a start and stop date

Figure 45. Rule Setup window—When tab



9. When you are finished configuring the workflow rules, click Save.

Modifying or Deleting a Workflow

Modifying or deleting a workflow goes into effect after the agents affected by the workflow log out and log back in to their Windows session.

If the agents do not log out of their Windows session, they continue to be recorded according to the workflow as it was before it was modified or deleted.

To modify a workflow:

1. Select the Workflows node in the navigation tree.
The Workflow Administration window is displayed.
2. Select the workflow from the Workflows pane to modify the assigned teams or the workflow settings.
Select the workflow under the Workflow node in the navigation tree to modify the workflow's classifiers, rules, and actions.
3. When you are finished making changes, click Save.

To delete a workflow:

1. Select the workflow in the navigation tree.
2. Click Delete.
3. Click Yes to confirm the deletion.
The workflow is deleted.

Evaluation Forms

6

Introduction

The Evaluation Forms section enables you to:

- Create and maintain evaluation forms
- Configure who can evaluate contacts that use a specific form
- Configure who can approve evaluations that use a specific form

New forms are created based on one of four read-only templates that come with QM Administrator.

Form Status

A form's status determines if it is available for use and if it can be modified. There are three statuses.

Table 15. Form statuses

Status	Description
Editable	The form can be modified, renamed, and deleted. It is not yet available for evaluators to use.
Active	The form is released to be used by evaluators. Only the Header information of the form can be modified. The form cannot be deleted.
Inactive	The form is removed from use by evaluators. It will be deleted automatically as soon as all evaluations based on it are removed from the database.

The normal lifecycle of an evaluation form is as follows:

Editable > Active > Inactive > Deleted

Once you have changed a status to the next in line, you cannot go back to the previous status. Also, you cannot skip a status (go from Editable to Inactive).

To change a form's status:

1. In the navigation tree, select Recordings > Evaluation Forms > Forms.
The Evaluation Form Administration page appears.
2. Select the form whose status you wish to change from the list of forms at the top of the page.
3. On the Properties tab, in the Status section, select the desired status (in accordance with the normal form lifecycle), and then click Save.

Creating an Evaluation Form

New evaluation forms are created based on one of the four templates that come with QM Administrator. Templates cannot be modified.

Table 16. Evaluation form templates

Template Name	Description
Blank Template 0-5	Configured for questions that are scored on a scale of 0 to 5. The template has no pre-existing sections or questions.
Blank Template Yes-No	Configured for questions that are answered with Yes or No. The template has no pre-existing sections or questions.
Template 0-5	Configured for questions that are scored on a scale of 0 to 5. The template comes with pre-existing sections and questions.
Template Yes-No	Configured for questions that are answered with Yes or No. The template comes with pre-existing sections and questions.

Creating an evaluation form involves the following steps:

- Creating a new form
- Configuring the form properties
- Configuring the form header information
- Configuring the form's sections
- Adding questions to each section

Creating a New Evaluation Form

To create a new evaluation form:

1. In the navigation tree, select Recordings > Quality Management > Evaluation Forms > Forms. The Evaluation Form Administration window appears (Figure 46).

Figure 46. Evaluation Form Administration window

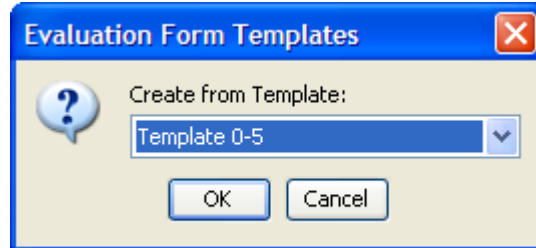
Name	Status	Type	Original Author	Last Author	Created	Modified
BvForm	Active	Yes-No	Administrator	Administrator	Jul 9, 2008	Jul 9, 2008

2. Click New. The Evaluation Form Name dialog box appears (Figure 47).

Figure 47. Evaluation Form Name dialog box

3. Enter a unique name for the new evaluation form and then click OK. The Evaluation Form Templates dialog box appears (Figure 48).

Figure 48. Evaluation Form Templates dialog box



4. Choose a template from the drop-down list, and then click OK. The new evaluation form is added to the list of forms at the top of the Evaluation Form Administration window.

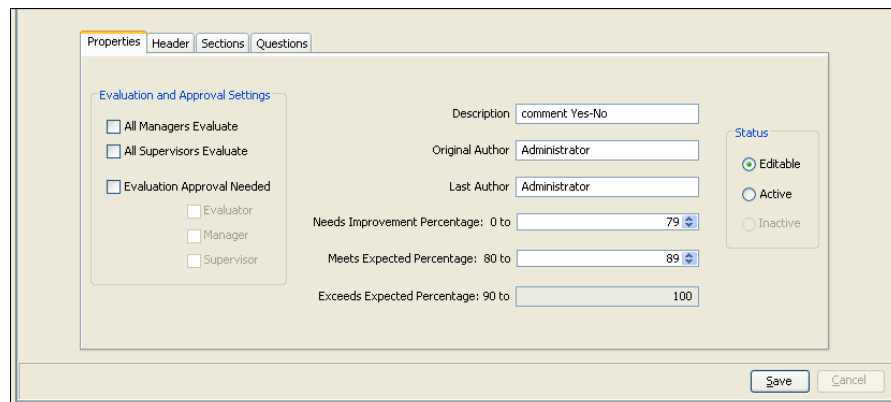
You can now configure the newly-created evaluation form by completing the information on each tab on the lower part of the window.

Properties Tab

To configure the form's properties:

1. Select the form in the list of forms at the top of the Evaluation Form Administration window. The form's properties are displayed in the tabbed section at the bottom of the window (Figure 49).

Figure 49. Properties tab



2. Select the Properties tab, and complete the fields as desired, or keep the default values.

Table 17. Properties Tab fields

Field	Description
Evaluation and Approval Settings	
All Managers Evaluate	Select this check box if you want all managers to be able to evaluate contacts that use this evaluation form and that are made by agents in their group.
All Supervisor Evaluate	Select this check box if you want all supervisors to be able to evaluate contacts that use this evaluation form and that are made by agents in their team.
Evaluation Approval Needed	Select this check box if you want to require evaluation approval for contacts that use this evaluation form. You can enable evaluation approval for some or all of the roles listed. Managers, supervisors, and evaluators will be able to approve evaluations for agents in their teams or groups.
Description	Descriptive name for the form. Default is the name of the template used to create the form.
Original Author	The name of the person who originally created the form. Default is Administrator.
Last Author	The name of the person who last updated the form. Default is Administrator.
Needs Improvement Percentage	The evaluation score range that indicates the agent's performance needs improvement. Default is 0–74%. If you change the value, all other score ranges change accordingly.
Meets Expected Percentage	The evaluation score range that indicates the agent's performance meets expectations. Default is 75–89%. If you change the value, all other score ranges change accordingly.
Exceeds Expected Percentage	The evaluation score range that indicates the agent's performance exceeds expectations. Default is 90–100%. This field is not editable. The value in it depends on the values set in the lower two score range fields.

Table 17. Properties Tab fields (cont'd)

Field	Description
Status	The default status is Editable. Do not change the status of the form to Active until you have completed setting it up. See "Form Status" on page 106 for more information on statuses.

3. When done, click Save.

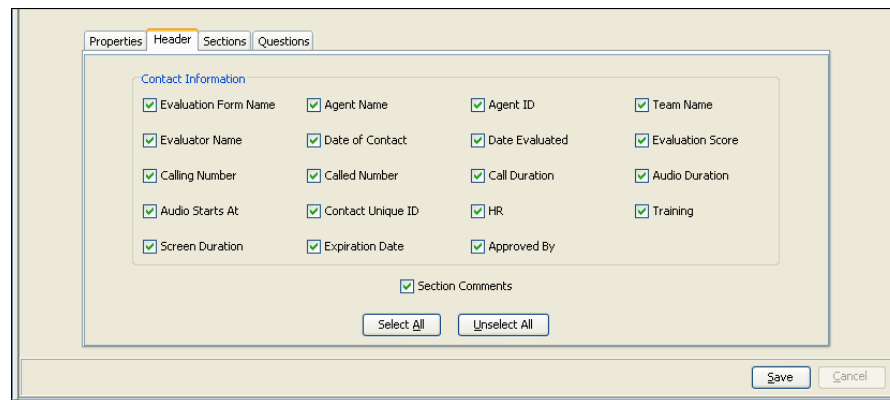
Header Tab

The header tab controls what contact information is displayed in the Evaluation View in QM Desktop and whether or not section comments are enabled for evaluations that use this form. This information can be edited no matter what the form's status is.

To configure the form header:

1. With the form selected in the form list, choose the Header tab ([Figure 50](#)).

Figure 50. Header tab



2. Select/deselect the information you want to appear, and then click Save.

Sections Tab

If you used the 0–5 Template or the Yes-No Template to create your new form, you already have sections set up. You can use these default sections as they are, or customize them to suit your needs by renaming them or deleting them.

If you used the Blank 0–5 Template or the Blank Yes-No Template, you will have to create sections.

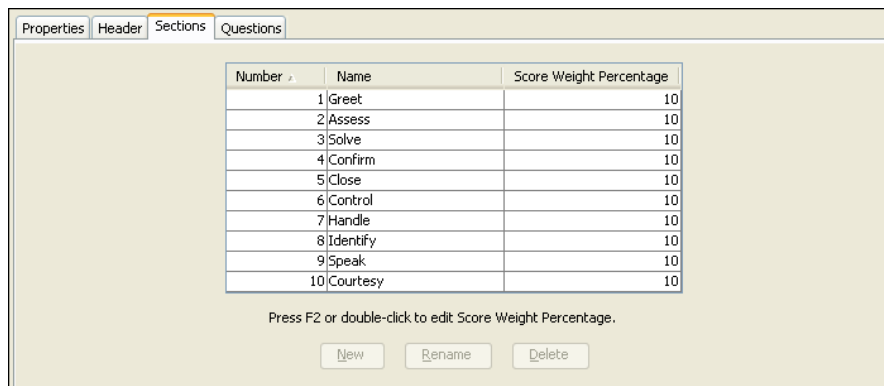
There can be a maximum of 10 sections in a form. The score weight percentages assigned to the sections must add up to 100 percent.

To add a new section:

1. With the form selected in the form list, select the Sections tab (Figure 51).
2. Click New. The Section Name dialog box appears.
3. Enter a name for the new section, and then click OK.

The new section is added to the list of sections. Sections are automatically numbered from 1 to 10.

Figure 51. Sections tab



4. Select the new section in the section list, and enter a score weight percentage for it in the Score Weight Percentage field. The total of all score weight percentages for the section must add up to 100 percent.
5. When you are finished adding new sections, click Save.

To rename a section:

- Select the section, click Rename, enter the new name in the Section Name dialog box, and then click OK.

To delete a section:

- Select the section, click Delete, and then confirm that you wish to delete the selected section.

NOTE: After deleting a section, the score weight percentages of the remaining sections will have to be changed so that they once again add up to 100 percent.

Questions Tab

If you used the 0–5 Template or the Yes-No Template to create your new form, you already have questions set up. You can use these default questions as they are, or customize them to suit your needs by adding, editing, or deleting questions.

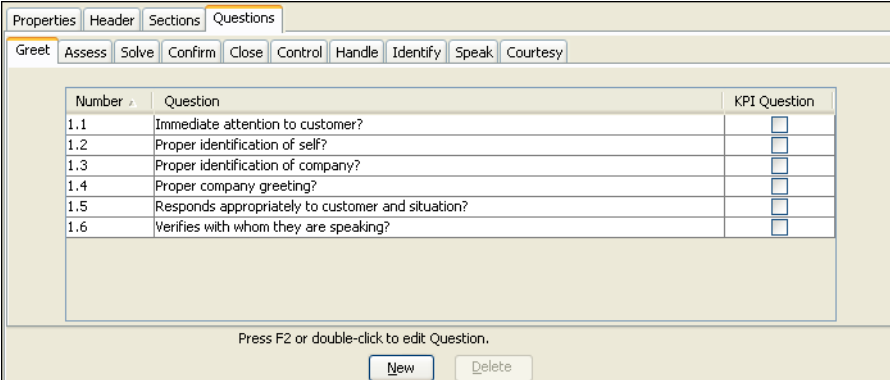
If you used the Blank 0–5 Template or the Blank Yes-No Template, you will have to create questions.

There can be a maximum of 10 questions in each form section.

To add a question:

1. With the form selected in the form list, select the Questions tab (Figure 52).

Figure 52. Questions tab



Number	Question	KPI Question
1.1	Immediate attention to customer?	<input type="checkbox"/>
1.2	Proper identification of self?	<input type="checkbox"/>
1.3	Proper identification of company?	<input type="checkbox"/>
1.4	Proper company greeting?	<input type="checkbox"/>
1.5	Responds appropriately to customer and situation?	<input type="checkbox"/>
1.6	Verifies with whom they are speaking?	<input type="checkbox"/>

Press F2 or double-click to edit Question.

New Delete

2. Select the Section tab to which you want to add questions, and then click New.

The New Question dialog box appears.

3. Type the new question, and then click OK.

The new question is added to the list of questions. Questions are automatically numbered from 1 to 10.

4. Select the KPI Question check box next to any question you want to designate as a Key Performance Indicator question. (See "[Key Performance Indicator \(KPI\) Questions](#)" for more information.)
5. When you are done adding questions, click Save.

To delete a question:

1. Select the question you want to delete, and then click Delete.
2. Click Save.

Key Performance Indicator (KPI) Questions

A key performance indicator (KPI) question is one that is so important that, if it is scored as a zero (for questions scored on a scale of 0–5) or No (for questions scored as Yes/No) the entire evaluation is automatically given a zero score. An example of a KPI question is “Did the agent refrain from using foul language?”

You can designate as many questions as you want as KPI questions, and anywhere questions appear in QM (for example, when reviewing an evaluation or viewing reports), KPI questions are identified as such.

Even though a KPI question forces an evaluation to an automatic zero score, the scores of all questions and sections are still available for viewing, and must be completed as normal.

Backup and Restore

7

Introduction

There are two situations in which QM data is backed up and restored.

- Upgrading your system from earlier versions of QM to QM 2.6
- Making a disaster recovery backup of version 2.6

Upgrades

When upgrading from version 2.3 or version 2.4 to version 2.6, the installation process automatically backs up your data and restores it to the newly-installed version 2.6. It is not necessary to manually backup and restore the data.

Disaster Recovery

You can back up and restore QM version 2.6 data using the BARS (backup and restore) command line utility that is installed with QM Administrator.

There are three QM databases, SQMDB, SQMReportDB, and hibernate. SQMReportDB and hibernate do not store historical data. Rather, they store configuration information needed to ensure that reports work correctly. They are created whenever the QM services are installed. Therefore the SQMReportDB and hibernate do not need to be backed up. If they are ever deleted, they can be reinstalled by running the QM Configuration Setup tool, “Create Database Catalogs” (see “QM Configuration Setup Tools” in the *Cisco Quality Management Installation Guide*).

In the rest of this chapter, a reference to the QM database means the SQMDB database and not the SQMReportDB or hibernate database.

BARS backs up and restores the LDAP and QM databases.

- The LDAP database is backed up to your local computer.

- The QM database is backed up to a folder on the computer that hosts Microsoft SQL Server.

NOTE: After you back up LDAP and QM, it is advisable to copy the backup files to another location for safekeeping.

BARS and Cisco Security Agent

If Cisco Security Agent (CSA) is present on a QM server, it can interfere with BARS and prevent a successful backup and restore. For this reason, it is necessary to stop CSA whenever you backup and restore data, and restart it when you are finished.

Command Line Syntax

The BARS utility uses the following syntax:

```
bars.exe [-BL | -RL | -BD | -RD] -d=<file path>]
```

The options are case sensitive. They are defined as follows:

Option	Description
-BL	Back up the LDAP database
-BD	Back up the QM database
-RL	Restore the LDAP database
-RD	Restore the QM database
-d=<path>	Path of the location where backup files are stored, if it is not the default location. This location must already exist—BARS will not create the folder location during the backup process. This command is required when backing up an external database location.

By default, the BARS utility is installed in the following location on the computers that host QM Administrator, the QM Database Service, and the LDAP Service:

```
C:\Program Files\Calabrio\WFO_QM\bin\bars.exe
```

Backing Up the LDAP and QM Databases

To back up the LDAP and QM databases:

1. On the computer that hosts the QM services, open a command window.

2. Navigate to the folder where the BARS utility is located and type:

```
bars.exe -BL -BD
```

3. Press Enter.

The utility creates the following backup files:

- A QM backup file named SQMdbbackup.dat located in the C:\Program Files\Common Files\SQM\backup\SQMdb folder on the computer that hosts the QM Database Services.
- A number of LDAP backup files located in the C:\Program Files\Common Files\SQM\backup\ldap folder on your local computer. The files are in XML format.

NOTE: It is recommended that you copy the backup files to a secure location for safekeeping.

Restoring the LDAP and QM Databases

It may become necessary to restore your QM system from the backup files due to database corruption or some other problem.

To restore the LDAP and QM databases:

1. Ensure that QM Administrator is closed.
2. Stop the following QM services:
 - Quality Management DB Cleaner Service
 - Quality Management DB Proxy Service
 - Quality Management Mana Service
 - Quality Management Sync Service
 - Quality Management Upload Controller Service
 - Quality Management Network Recording Service
 - Quality Management Monitor Service
 - Tomcat on the Voice, Screen, and Base servers
3. On the computer that hosts QM Administrator, open a command window.
4. Navigate to the folder where the BARS utility is located and type:

```
bars.exe -RL -RD -d=<path>
```

NOTE: Use the `-d=<path>` option only if you moved the backup files to a location other than the default location (C:\Program

Files\Common Files\SQM\backup\). If the files are in the default backup location, you do not need to include this option.

5. Press Enter.

The LDAP and QM databases are restored.

6. Restart the QM services you stopped in Step 2.

Index

-
- A**
- Archive recordings 87
 - Assigning roles 73
- B**
- Backup and Restore (BARS) utility 115
 - backing up LDAP and QM databases 116
 - command line syntax 116
 - restoring LDAP and QM databases 117
- C**
- CDR information formats 44
 - Changing form status 106
 - Changing password 10
 - Cisco Unified CC Database window 19
 - Cisco Unified CM window 21
- D**
- Databases
 - backing up 116
 - restoring 117
 - synchronizing 11
- E**
- Enterprise Settings window 19
 - adding Active Directory domain 26
 - Evaluation forms
 - adding questions 113
 - adding sections 112
 - creating 107
 - deleting questions 113
 - deleting sections 112
- F**
- header 111
 - properties 109
 - questions 113
 - renaming sections 112
 - sections 111
 - status 106
 - templates 107
 - Exporting a recording 89
 - Extended screen recording 99
 - External API 8
- G**
- Form header 111
 - Form status 106
 - changing 106
- I**
- Inclusion List window 46
 - adding extensions 47
 - excluding extensions 47
 - Interface 14
- L**
- Licenses 27
 - Logging in 9
 - Logging out 12
- L**
- Group administration
 - adding a group 77
 - assigning teams and managers 78

M

- Managers, assigning to group 78
- Metadata, user-defined 84
 - configuring 90
- Monitoring and Notification window 33

N

- New workflows 95
- Notification trigger reports 44
- Notification triggers 39

Q

- QM Administrator
 - changing password 10
 - interface 14
 - logging in 9
 - logging out 12
 - navigation 14
 - what's new in this version 7
- QM Databases window 23
- QM users 69
 - creating 72
- Quality Management API 8
- Quality management recordings 83
 - retention periods 85

R

- Recordings
 - exporting 89
 - extended screen 99
 - introduction 83
 - quality management 83
 - retention periods 85
- Reports, notification trigger 44
- Roles 73

S

- Saving a recording 89
- Site configuration
 - Cisco Unified CC Database window 19
 - Cisco Unified CM window 21
 - Enterprise Settings window 19
 - Inclusion List window 46
 - introduction 17
 - licenses 27
 - modifying information 18
 - Monitoring and Notification window 33

- QM Databases window 23
- Status window 49
- Upload Settings window 31
- Sorting tables 15
- Status window 49
- Synchronizing databases 11

T

- Tables, sorting 15
- Teams, assigning to group 78

U

- Upload Settings window 31
- User administration 62
- User Administration window 63, 69
- User-defined metadata 84, 90

W

- What's new in this version 7
- Workflows
 - configuring actions 98
 - creating new 95
 - deleting 103
 - modifying 103
 - overview 93
 - setting up classifiers 96
 - setting up rules 99
 - What tab 100
 - When tab 102
 - Who tab 101