Contents

Overview 13

- Quality Management Components 13
  Client Applications 13
    Quality Management Administrator 13
    Calabrio Screen Player Plug-in 13
    Desktop Recording Service 14
  Web Applications 14
    Cisco Unified Workforce Optimization 14
  Services 14
    Quality Management CTI Service 14
    Quality Management Data API Service 14
    Quality Management DB Cleaner Service 14
    Quality Management DB Proxy Service 15
    Quality Management Jetty Service 15
    Quality Management Monitoring and Notification Service 15
    Quality Management Monitor Service 15
    Quality Management Network Recording Service 15
    Quality Management Sync Service 15
    Quality Management Upload Controller 15

- Mixed Mode Licensing 16
  Quality Management License 16
    Advanced Quality Management License 16
    Call Recording License 16

- System Configuration 17
  Supported Configuration 18

- System Requirements 18
  System Environment 19
    Unified CCX System Environment 19
  Data Configuration Environment 19
  Operating Environment 20
    Cisco Unified Workforce Optimization and/or Quality Management Administrator (No Recording) 20
    QM License and Call Recording License (Voice Recording Only) 21
    QM License and Call Recording License (Voice Recording Plus) 22
    AQM License (Voice and Screen Recording) 23
Prerequisites 51

• Pre-installation and Deployment Checklists 51
• Microsoft Server 2008 51
  Enabling Desktop Experience on Windows Server 2008 51
• Microsoft SQL Server 52
  Installing Microsoft SQL Server 52
  Creating an SQL Server User Login for Initial Installation 54
  Configuring Microsoft SQL Server for Quality Management 55
    Microsoft SQL Server 2008 Requirements 55
    Adding Firewall Exclusions by Application 55
    Allowing Remote Connections 56
    Configuring the SQL Server Browser 57
  Microsoft SQL Roles 57
  Creating an SQL Server User Login for Initial Installation 58
Creating an SQL Server User Login for Upgrades 58
• Windows SNMP Services 59
  Installing Windows SNMP Services 60
• JTAPI User 60
• Active Directory 61
  Active Directory Configuration Guidelines 61
  Active Directory Information 62
  Locating the Active Directory Domain Name 62

Installing Quality Management 63
• Services for Quality Management 63
  Installing Services 63
• Supporting Asian Languages 65
  Installing Supplemental Language Support 65
• Installing Client Applications for Quality Management 66
  Enabling the Elevated Privileges Policy for Window Installer Installation 67
  Enabling the Windows Elevated Privileges Policy 67
  Installing Client Applications for Quality Management 68
  Calabrio Screen Player Plug-in Limitations 68
  Enabling the Next Generation Java Plug-in 68
• Using Automated Package Distribution Tools 69
  Requirements 69
    Execution 69
    Per-Machine vs. Per User 69
    Privileges 69
    Automated Package Installation vs. Manual Installation 70
    Multiple Software Releases 70
    Reboots 70
  Best Practices 71
    Windows Installer Logging 71
    Deployment 71
    Installation and Uninstallation Deployment Packages 71
Recommended Deployment Preparation Model 71
Client Installation Packages on the Installation DVD 72
Running Site Configuration Setup 73

- Entering Configuration Data in Initial Mode 73
  Manually Installing the Cisco JTAPI Client 80
- Site Configuration Setup Steps 81
- Quality Management Database 81
  Configuration Settings Used By Services 82
- Cisco Unified CC Database 82
  Configuration Settings Used By Services 85
- Cisco Unified CM 86
  Configuration Settings Used By Services 88
  Adding a Unified CM Cluster 88
  Deleting a Unified CM Cluster 89
- Quality Management CTI Service 90
  Configuration Settings Used By Services 91
  Adding a Backup CTI Service 92
- Enterprise Settings 93
  Configuration Settings Used By Services 94
  Software Updates 95
  Session Timeout Options 95
  License 96
    Importing a License File 97
    Licensing Rules 98
  Active Directory 98
    Adding an Active Directory Domain 101
  Removing an Active Directory Domain 102
- Locale 102
  Enabling a Locale 102
- Recording File Storage Location 102
  Configuring the Recording Location 105
- Upload Settings 106
  Configuration Settings Used By Services 108
- Monitoring and Notification 108
  Configuration Settings Used By Services 111
Configuring the SNMP Settings 111
Using Email Addresses for Notification 112
  Configuring the SMTP Settings for Email 113
  Adding a Notification Email Address 114
Using Notification Triggers 115
  CDR Information Formats for the QM3002 Notification Trigger 116
  Summary Only 116
  Detail (Tab Delimited) 117
  Detail (Plain Text) 117
  Enabling or Disabling a Notification Trigger 118
  Configuring the QM3002 Notification Trigger 119
  Adding an Ignored Extension 120
  Modifying an Ignored Extension 120
  Removing an Ignored Extension 121
  Examples of Notification Configuration Problems 121
• RTP Filters 123
  Configuration Settings Used By Services 124
  RTP Filter Guidelines 124
  Adding an RTP Filter 125
  Editing an RTP Filter 125
  Deleting an RTP Filter 126
• Status 127
  Configuration Settings Used By Services 127
• Entering Configuration Data in Update Mode 127
  Rules for Upgrading or Modifying the Unified CC Database in Update Mode 127
  Stopping the Sync Service Before Upgrading the Unified CCX Database 128
  Changing the Base Server 128
  Changing Quality Management Configuration Data in Update Mode 129
• Site Configuration Setup Tools 130
  Start Local Services 131
  Create Database Catalogs 132
  Generate Info for MSI Clients 132
  Download/Install JTAPI 132
  Encrypt Audio Files 132
  Set Recording Home Directory 132
Changing the Recording Location in Update Mode 133
Generate SSL Certificate 133
Test CTI Service(s) 134
Display Metadata Encryption Key 134
Choose Monitor Adaptor 134
Remove Recording Services 134
Configure Local Servers 134

Setting Up NT Authentication for the Cisco Unified CC Database 135
• Setting Up NT Users 135
  Adding an NT User 135
  Adding an NT User to a Group 136
• Verifying the Connection 136
• Allowing the User Access to the Cisco Unified CC Database 136

Supporting Asian Languages 139
• Installing Supplemental Language Support 139

Upgrading from Previous Versions 141
• Workflows and Retention Periods 141
• Upgrade Guidelines 142
  NT Authentication 142
  PrgpxNT.dll Failed to Register 142
• Upgrading Quality Management 8.0(2) to Quality Management 8.5 143
• Upgrading Quality Management 2.6 or 2.7 to Quality Management 8.5 144
• Upgrading the Client Applications 145
• Testing the Upgrade on Client Machines 145
• Verifying the Upgrade is Installed Correctly on the Quality Management Server 146
Installing a Service Release or Patch 147

- Guidelines for Installing a Patch (SR or ES) 148
- Installing an Patch (ES or SR) 148
- Rolling Back to a Previous State 149

Removing Quality Management 2.6 or 2.7 151

- Removing a Quality Management Application 152
- Removing the Quality Management Databases 152
- Verifying Quality Management was Removed Correctly 154

Removing Quality Management 8.5 155

- Removing a Quality Management Application 156
- Removing the Quality Management Databases 156

Checklists and Activities 159

- Pre-Installation Checklists 159
  - Pre-installation Checklist 159
  - Pre-order Validation Checklist 160
  - Environment Information Checklist 161
  - IP Phone Models and Remote Access Checklist 161
  - Base Server Information Checklist 162
  - Cisco Unified CC Database Checklist 162
  - Cisco Unified CM Information Checklist 163
  - SQL Server Checklist 163
  - SQL Database Server Information 164
  - Quality Management CTI Service Information 164
  - Enterprise Settings Information Checklist 165
  - Active Directory Domain Information Checklist 165
Backup and Restore 185

• Upgrades  185
• Disaster Recovery  185
• Backing Up the Quality Management Databases  185
• Restoring the Quality Management Database  186
Overview

This document explains how to install Cisco Unified Workforce Optimization Quality Management 8.5.

Install Quality Management 8.5 in the following order:

1. Prepare the server for Quality Management installation
2. Install and configure Quality Management on the server component
3. Install Quality Management Administrator to configure users, groups, workflows, and other Quality Management elements
4. Install the Calabrio Screen Player Plug-in on client PCs
5. Install the Desktop Recording service on client PCs
6. Verify agents can access Cisco Unified Workforce Optimization

Quality Management Components

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

Client Applications

You can install the Quality Management client applications from web pages. These web pages reside on the Quality Management Base Services server.

Quality Management Administrator

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

You install Quality Management Administrator on the client PC assigned to the Quality Management administrator.

Calabrio Screen Player Plug-in

Use the Calabrio Screen Player Plug-in to play back recordings from the Search and Play widget and the Evaluate and Review widget in the Cisco Unified Workforce Optimization.

You install Calabrio Screen Player Plug-in on client PCs.
**Desktop Recording Service**

The Desktop Recording service, located on the agent's PC, is responsible for recording contacts and collecting metadata associated with recorded calls.

The Desktop Recording service uploads recordings to the Voice and Screen server and uploads the metadata to the Quality Management database. See “Desktop Recording Service (Endpoint) Requirements” on page 42 for more information.

You install Desktop Recording services on client PCs.

**Web Applications**

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

**Cisco Unified Workforce Optimization**

Use Cisco Unified Workforce Optimization to evaluate contacts, view evaluated contacts, view reports, and access archived contacts. Each user role has a different level of access to information.

**Services**

You install the following services for Quality Management from the Quality Management DVD.

**Quality Management CTI Service**

The Quality Management CTI service (CTI service) acts as a bridge between the Desktop Recording service and Cisco Unified Communications Manager/CTI Manager. The Quality Management CTI service sends events to the Desktop Recording service when there is a change in the status of monitored phones. The CTI service is part of CTI Services.

**Quality Management Data API Service**

Quality Management components use the Quality Management Data API (Data API) service to get configuration data. This service also handles product-specific authentication and requests. The Data API service is part of Base Services.

**Quality Management DB Cleaner Service**

The Quality Management DB Cleaner (DB Cleaner) service purges records from the Quality Management database and purges media files from the Voice and Screen server on a daily basis. The retention time configured in Quality Management Administrator determines the time when the DB Cleaner service purges records. The DB Cleaner service is part of Database Services.
Quality Management DB Proxy Service

In Quality Management deployments, the Quality Management DB Proxy (DB Proxy) service is the single point of connection to the Recording Services database for both the DB Cleaner and Upload Controller services. The DB Proxy service is part of Database Services.

Quality Management Jetty Service

The Quality Management Jetty (Jetty) service webserver hosts the Quality Management Reports webapp, C1Surrogate webapp, File Transfer Servlet (FTS), Server API engine, and Licensing webapp. These applications are installed as part of Base Services and when you select Quality Management Voice/Screen Services during installation. The Jetty service is part of Base Services and Voice/Screen Services.

Quality Management Monitoring and Notification Service

The Quality Management Monitoring and Notification (Mana) service handles real-time monitoring of the Quality Management system. When there are problems, the Mana service notifies the administrators through the event viewer, email, or SNMP. You can select the problems that trigger the notification in Quality Management Administrator. The Mana service is part of Base Services.

Quality Management Monitor Service

The Quality Management Monitor (Monitor) service works in conjunction with the Network Recording service for server recording. The Monitor service captures the packets that the Network Recording service records. You can use this primarily in instances where Desktop Recording (Endpoint) is not supported. The Monitor service is part of Monitor Services and Quality Management.

Quality Management Network Recording Service

The Quality Management Network Recording (Network Recording) service enables recording for agents who are configured for Server Recording and Network Recording. You can configure a mix of devices associated with the same server running the Network Recording service for Server Recording and Network Recording. The Network Recording service (RecordServer.exe) is part of the Recording Services component only.

Quality Management Sync Service

The Quality Management Sync (Sync) service synchronizes the data every 10 minutes from Unified CCX to the Quality Management database. The Sync service is part of Base Services.

Quality Management Upload Controller

The Quality Management Upload Controller (Upload Controller) service manages the upload of recordings to the Voice and Screen Server and records metadata to the
Mixed Mode Licensing

You need to assign licenses to the following users.

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

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

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

When you log into Workforce Optimization, you have access to all applications allowed by the license and roles assigned to you. For example, if a supervisor has only the CR license, the supervisor cannot evaluate a recording in the Recordings application. However, the supervisor can access Recordings application. If that same supervisor finds a screen recording via the Recordings application, the supervisor can in fact play that screen recording.

Quality Management License

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

Advanced Quality Management License

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

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

Call Recording License

The Cisco Unified Workforce Optimization Call Recording (CR) license allows only audio recording and archive search and playback. Status and archive reports are available to supervisors and managers only.
System Configuration

This topic describes the system configuration for Quality Management.

Quality Management supports one system configuration. This configuration is able to use an optional external storage server to store voice and screen recording files. Figure 1 on page 18 illustrates the supported configuration.

The single server configuration consists of the following servers.

• Quality Management
  – CTI service
  – Data API service
  – DB Cleaner service
  – DB Proxy service
  – Jetty service
  – Mana service
  – Monitor service (for Server Recording or Network Recording)
  – Network Recording service (for Server Recording or Network Recording)

  **NOTE:** The Monitor service and the Network Recording services are optional services. You can choose to install these services on the Base Services server or separate servers.

  – Sync service
  – Upload Controller

• Optional external recording storage server

• Optional external server hosting SQL server

  **NOTE:** Screen recording is available to users who have the Advanced QM license only.

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

![Supported configuration](image)

System Requirements

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

Quality Management 8.5 supports the Cisco Unified Contact Center Express (Unified CCX) environment.

Unified CCX System Environment

Quality Management supports the following Cisco Unified CCX and Unified Communications Manager (CM) version combinations:

<table>
<thead>
<tr>
<th>Cisco Unified CCX</th>
<th>Cisco Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5(x) all SUs</td>
<td>8.5(1) all SUs, 8.0(x) all SUs</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Quality Management does not support Cisco Unified CM 8.6.</td>
</tr>
</tbody>
</table>

**NOTE:** Quality Management has direct dependencies on Cisco Unified CM for CTI and SIP events and that is why Quality Management compatibility with Unified CM is listed in this *Installation Guide*. Do not assume Quality Management is compatible with all version of Unified CM that are listed as compatible with versions of Unified CCX within the Cisco Unified Contact Center Express Compatibility Information on the Cisco website (www.cisco.com).

Data Configuration Environment

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

Operating Environment

Quality Management 8.5 runs in the operating environment described in Table 2 through Table 7 on page 25.

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

Table 2 displays the minimum hardware requirements for Cisco Unified Workforce Optimization and/or Quality Management Administrator without recording.

Table 2. Cisco Unified Workforce Optimization and/or Quality Management Administrator (no recording)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
</table>
| Windows XP Professional, Service Pack 3 or later | 1 GHz processor  
256 MB RAM  
200 MB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024  
screen resolution Medium (16 bit) 65,000 colors minimum |
| Windows Vista Business, Enterprise, and Ultimate Editions\(^b\), Service Pack 2 | 1 GHz processor  
1 GB of system memory  
200 MB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024  
screen resolution Medium (16 bit) 65,000 colors minimum |
| Windows 7 Professional and Ultimate\(^c\) | 1 GHz processor  
1 GB of system memory  
200 MB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024  
screen resolution Medium (16 bit) 65,000 colors minimum |

\(^a\) NICs must support Promiscuous Mode. See the Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring documents for more information on the Promiscuous Mode and testing a NIC’s capabilities. These documents are available on the Cisco website. Note that the Cisco website is subject to change without notice. If the above links do not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.

\(^b\) Quality Management does not support 64-bit processor for Vista. The latest Microsoft Vista requirements are available at: http://www.microsoft.com/windows/windows-vista/get/system-requirements.aspx

**QM License and Call Recording License (Voice Recording Only)**

Table 3 displays the minimum hardware requirements for QM License and Call Recording License for voice recording only.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional, Service Pack 3 or later</td>
<td>500 MHz processor, 256 MB RAM, 1 GB HDD free space, 100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Windows Vista Business, Enterprise, and Ultimate Editions&lt;sup&gt;b&lt;/sup&gt;, Service Pack 2</td>
<td>1 GHz processor, 1 GB of system memory, 1 GB HDD free space, 100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Windows 7 Professional and Ultimate&lt;sup&gt;c&lt;/sup&gt;</td>
<td>1 GHz processor, 1 GB of system memory, 1 GB HDD free space, 100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

a. NICs must support Promiscuous Mode. See the Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring documents for more information on the Promiscuous Mode and testing a NIC’s capabilities. These documents are available on the Cisco website. Note that the Cisco website is subject to change without notice. If the above links do not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.


**QM License and Call Recording License (Voice Recording Plus)**

Table 4 displays the minimum hardware requirements for QM license and Call Recording license with voice recording plus Cisco Unified Workforce Optimization and/or Quality Management Administrator.

Table 4. QM license and Call Recording license (voice recording plus Cisco Unified Workforce Optimization and/or Quality Management Administrator)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional, Service Pack 3 or later</td>
<td>1 GHz processor&lt;br&gt;256 MB RAM&lt;br&gt;1 GB HDD free space&lt;br&gt;100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;&lt;br&gt;1280 x 1024&lt;br&gt;screen resolution Medium (16 bit) 65,000 colors minimum</td>
</tr>
<tr>
<td>Windows Vista Business, Enterprise, and Ultimate Editions&lt;sup&gt;b&lt;/sup&gt;, Service Pack 2</td>
<td>1 GHz processor&lt;br&gt;1 GB of system memory&lt;br&gt;1 GB HDD free space&lt;br&gt;100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;&lt;br&gt;1280 x 1024&lt;br&gt;screen resolution Medium (16 bit) 65,000 colors minimum</td>
</tr>
<tr>
<td>Windows 7 Professional and Ultimate&lt;sup&gt;c&lt;/sup&gt;</td>
<td>1 GHz processor&lt;br&gt;1 GB of system memory&lt;br&gt;1 GB HDD free space&lt;br&gt;100 Mbit NIC&lt;sup&gt;a&lt;/sup&gt;&lt;br&gt;1280 x 1024&lt;br&gt;screen resolution Medium (16 bit) 65,000 colors minimum</td>
</tr>
</tbody>
</table>

<sup>a</sup> NICs must support Promiscuous Mode. See the Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring documents for more information on the Promiscuous Mode and testing a NIC’s capabilities. These documents are available on the Cisco website. Note that the Cisco website is subject to change without notice. If the above links do not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.

<sup>b</sup> Quality Management does not support 64-bit processor for Vista. The latest Microsoft Vista requirements are available at: http://www.microsoft.com/windows/windows-vista/get/system-requirements.aspx

<sup>c</sup> Quality Management does not support 64-bit processor for Windows 7. The latest Microsoft Windows 7 requirements are available at http://windows.microsoft.com/systemrequirements.
### AQM License (Voice and Screen Recording)

Table 5 displays the minimum hardware requirements for AQM License using voice and screen recording.

**Table 5.** AQM License (voice and screen recording)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional, Service Pack 3 or later</td>
<td>1.4 GHz processor</td>
</tr>
<tr>
<td></td>
<td>1 GB RAM</td>
</tr>
<tr>
<td></td>
<td>1 GB HDD free space</td>
</tr>
<tr>
<td></td>
<td>100 Mbit NIC(^a)</td>
</tr>
<tr>
<td>Windows Vista Business, Enterprise, and Ultimate Editions(^b), Service Pack 2</td>
<td>2 GHz processor</td>
</tr>
<tr>
<td></td>
<td>2 GB of system memory</td>
</tr>
<tr>
<td></td>
<td>1 GB HDD free space</td>
</tr>
<tr>
<td></td>
<td>100 Mbit NIC(^a)</td>
</tr>
<tr>
<td>Windows 7 Professional and Ultimate(^c)</td>
<td>2 GHz processor</td>
</tr>
<tr>
<td></td>
<td>2 GB of system memory</td>
</tr>
<tr>
<td></td>
<td>1 GB HDD free space</td>
</tr>
<tr>
<td></td>
<td>100 Mbit NIC(^a)</td>
</tr>
</tbody>
</table>

\(^a\) NICs must support Promiscuous Mode. See the Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring documents for more information on the Promiscuous Mode and testing a NIC's capabilities. These documents are available on the Cisco website. Note that the Cisco website is subject to change without notice. If the above links do not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.

\(^b\) Quality Management does not support 64-bit processor for Vista. The latest Microsoft Vista requirements are available at http://www.microsoft.com/windows/windows-vista/get/system-requirements.aspx

\(^c\) Quality Management does not support 64-bit processor for Windows 7. The latest Microsoft Windows 7 requirements are available at http://windows.microsoft.com/systemrequirements.
### AQM License (Voice and Screen Recording Plus)

Table 6 displays the minimum hardware requirements for AQM License using voice and screen recording plus Cisco Unified Workforce Optimization and/or Quality Management Administrator.

Table 6. AQM License (voice and screen recording plus Cisco Unified Workforce Optimization and/or Quality Management Administrator)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
</table>
| Windows XP Professional, Service Pack 3 or later | 1.4 GHz processor  
1 GB RAM  
1 GB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024 screen resolution Medium (16 bit) 65,000 colors minimum |
| Windows Vista Business, Enterprise, and Ultimate Editions\(^b\), Service Pack 2 | 2 GHz processor  
2 GB of system memory  
1 GB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024 screen resolution Medium (16 bit) 65,000 colors minimum |
| Windows 7 Professional and Ultimate\(^c\) | 2 GHz processor  
2 GB of system memory  
1 GB HDD free space  
100 Mbit NIC\(^a\)  
1280 x 1024 screen resolution Medium (16 bit) 65,000 colors minimum |

\(^a\) NICs must support Promiscuous Mode. See the Configuring and Troubleshooting VoIP Monitoring and Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring documents for more information on the Promiscuous Mode and testing a NIC’s capabilities. These documents are available on the Cisco website. Note that the Cisco website is subject to change without notice. If the above links do not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.

\(^b\) Quality Management does not support 64-bit processor for Vista. The latest Microsoft Vista requirements are available at: http://www.microsoft.com/windows/windows-vista/get/system-requirements.aspx

\(^c\) Quality Management does not support 64-bit processor for Windows 7. The latest Microsoft Windows 7 requirements are available at http://windows.microsoft.com/systemrequirements.
Quality Management Base Server Operating Systems and Hardware Requirements

Table 7 displays the minimum hardware requirements for the Quality Management base server operating systems.

Table 7. Quality Management base server operating systems and hardware requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 Serverabc</td>
<td>Cisco Media Convergence Server (MCS) platform or exact equivalentd</td>
</tr>
<tr>
<td>Release 2</td>
<td></td>
</tr>
<tr>
<td>Service Pack 2</td>
<td></td>
</tr>
<tr>
<td>MSXML 6.0</td>
<td></td>
</tr>
<tr>
<td>5 Client Access Licenses (CAL)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Media Convergence Server (MCS) platform or exact equivalentd</strong></td>
</tr>
<tr>
<td>Windows 2008 Server R1bc</td>
<td></td>
</tr>
<tr>
<td>Service Pack 1</td>
<td></td>
</tr>
<tr>
<td>5 Client Access Licenses (CAL)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Media Convergence Server (MCS) platform or exact equivalentd</strong></td>
</tr>
<tr>
<td>VMware ESX Serverbcef</td>
<td>3.4 GHz Dual Pentium 4</td>
</tr>
<tr>
<td></td>
<td>3 GB RAM</td>
</tr>
<tr>
<td></td>
<td>200 GB RAM hard disk space</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Media Convergence Server (MCS) platform or equivalent</strong></td>
</tr>
</tbody>
</table>


b. Cisco only supports the English locale on the server’s operating system.

c. Cisco only supports the 32-bit version of Windows 2003 Server SP 2, Windows 2008 Server SP 1, and VMware ESX Server.


e. Cisco only tested Quality Management hosted on VMware for functionality. Cisco did not test for performance or scalability in the VMware environment. Due to the many VM configuration factors and possible performance impacts of additional hosted virtual servers, determining the actual server performance results under the VMware environment is the customer’s responsibility. If a problem occurs, the customer may be required to shut down other VM sessions or reproduce the problem in a non-VMware configuration to assist in the isolation of the issue. Cisco support for performance and scalability issues are limited to server-based deployments.

f. The Monitor Server is not supported on a virtual platform. The Monitor Server must be run on a physical machine.
Quality Management Base Server Operating Systems and Cisco Unified Computing System Hardware Requirements

The Quality Management Base server and Network Recording service are fully supported for installation and execution on the Cisco Unified Computing System (UCS) C series C210 and C200. The VM profile requires the following hardware.

- 2 vCPU
- 2 GB RAM
- 80 GB vDisk
- 1 vNIC

This profile is designed to support up to four VMware server instances running concurrently on a UCS C210M2 platform.

The server capacity, in terms of the number of named or concurrent users or recordings, is equal to the capacities shown in “Server Capacity Guidelines” on page 26 for the MCS 7845 equivalent server.

Server Capacity Guidelines

Use the capacity guidelines in the following table to determine the MCS server or MCS server equivalent to use as the as the server. You can also choose to configure MCS servers for Quality Management storage.

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

Server Specifications

Table 8 displays the server specifications.

Table 8. Server specifications

<table>
<thead>
<tr>
<th>Cisco MCS Equivalent</th>
<th>MCS 7816</th>
<th>MCS 7825</th>
<th>MCS 7835</th>
<th>MCS 7845</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Celeron D 352 3.2 GHz</td>
<td>Intel Dual-Core Xeon 3050 2.13 GHz</td>
<td>Intel 5140 Xeon 2.33 GHz</td>
<td>2x Intel 5140 Xeon 2.33 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>System Storage</td>
<td>40 GB</td>
<td>40 GB</td>
<td>40 GB</td>
<td>40 GB</td>
</tr>
<tr>
<td>Recording Storage</td>
<td>Varies by use</td>
<td>Varies by use</td>
<td>Varies by use</td>
<td>Varies by use</td>
</tr>
</tbody>
</table>
**Single Server Configurations for Server Recording and Network Recording**

Table 9 displays the capacity guidelines for a single server configuration where Server Recording (SPAN) or Network Recording are co-resident with (or hosted on the same server as) the Quality Management Base Services.

**Table 9. Single server configurations for Server Recording and Network Recording**

<table>
<thead>
<tr>
<th>Cisco MCS Equivalent</th>
<th>MCS 7816</th>
<th>MCS 7825</th>
<th>MCS 7835</th>
<th>MCS 7845</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of concurrent agents/users for voice only</td>
<td>n/a</td>
<td>40</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice and screen</td>
<td>n/a</td>
<td>20</td>
<td>35</td>
<td>50</td>
</tr>
</tbody>
</table>

See “Recording Storage Requirements for Server Recording and Network Recording” on page 31 for additional information on storage requirements.

**Single Server Configurations for either Desktop Recording or Off-board Server Recording or Network Recording**

Table 10 displays the capacity guidelines for a single server configuration using either Desktop Recording or off-board Server Recording or Network Recording.

**Table 10. Single server capacity guidelines for Desktop Recording**

<table>
<thead>
<tr>
<th>Cisco MCS Equivalent</th>
<th>MCS 7816</th>
<th>MCS 7825</th>
<th>MCS 7835</th>
<th>MCS 7845</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum number of named users for voice and screen recording</td>
<td>450</td>
<td>900</td>
<td>1500</td>
<td>3600</td>
</tr>
<tr>
<td>maximum number of concurrent agents/users for voice and screen recording</td>
<td>150</td>
<td>300</td>
<td>500</td>
<td>1200</td>
</tr>
</tbody>
</table>

Cisco requires an external SQL database server when Quality Management is configured for 500 or more users.

See “Recording Storage Requirements for Server Recording and Network Recording” on page 31 for additional information on storage and external database requirements.
Off-board Server Configurations for Network Recording

Table 11 displays the capacity guidelines for an off-board server configuration using Network Recording.

Table 11. Off-board server configurations for Network Recording

<table>
<thead>
<tr>
<th>Cisco MCS Equivalent(^a)</th>
<th>MCS 7816</th>
<th>MCS 7825</th>
<th>MCS 7835</th>
<th>MCS 7845</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of concurrent agents/users for voice only (Recording Server)</td>
<td>n/a</td>
<td>120</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice and screen (Recording Server)</td>
<td>n/a</td>
<td>60</td>
<td>100</td>
<td>150</td>
</tr>
</tbody>
</table>

\(^a\) A Monitor Server is not required for Network Recording.

See “Recording Storage Requirements for Server Recording and Network Recording” on page 31 for additional information on storage requirements.
Off-board Server Configurations for Server Recording

Table 12 displays the capacity guidelines for an off-board server configuration using Server Recording (SPAN).

Table 12. Off-board server configurations for Server Recording (SPAN)

<table>
<thead>
<tr>
<th>Cisco MCS Equivalent</th>
<th>MCS 7816</th>
<th>MCS 7825</th>
<th>MCS 7835</th>
<th>MCS 7845</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agents/users for voice only</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice only (Recording Server)</td>
<td>n/a</td>
<td>120</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice monitoring (Monitor Server)</td>
<td>n/a</td>
<td>80</td>
<td>130</td>
<td>200</td>
</tr>
<tr>
<td><strong>Agent/users for voice and screen</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice and screen (Recording Server)</td>
<td>n/a</td>
<td>60</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>Maximum number of concurrent agents/users for voice monitoring (Monitor Server)</td>
<td>n/a</td>
<td>80</td>
<td>130</td>
<td>200</td>
</tr>
</tbody>
</table>

See “Recording Storage Requirements for Server Recording and Network Recording” on page 31 for additional information on storage requirements.
Base Server Configuration

Figure 2 displays a base server configuration with optional SQL, redundant CTI, and recording services.

**Figure 2.** Quality Management Base server configuration with optional SQL, redundant CTI, and recording services
Recording Storage Requirements for Server Recording and Network Recording

Table 13 displays the Server Recording server and Network Recording server storage requirements. The recording storage requirements specify the amount of disk space required per recorded user for caching the recordings prior to their eventual upload to the Quality Management server.

Table 13. Recording Storage Requirements

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Storage Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Voice Only</td>
</tr>
<tr>
<td>Server Recording</td>
<td>.5 GB/recorded user</td>
</tr>
<tr>
<td>Network Recording</td>
<td>.5 GB/recorded user</td>
</tr>
</tbody>
</table>

Quality Management Storage Calculator

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


Disk Storage Sizing Guidelines

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

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

The number of minutes that will be recorded every day is the product of three numbers: the number of agents being recorded, the average call length, and the average number of calls that are recorded for each agent per day.
To estimate the amount of disk storage required for your system, use the following formulas:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily recorded minutes</td>
<td>Agents × Length × Calls = Recorded</td>
</tr>
<tr>
<td>Total recorded minutes to store</td>
<td>Recorded × Days × Months = Stored</td>
</tr>
<tr>
<td>Voice recording storage (MB)</td>
<td>Stored × 0.12 MB/minute = Voice</td>
</tr>
<tr>
<td>Screen recording storage (MB)</td>
<td>Stored × 1.20 MB/minute = Screen</td>
</tr>
</tbody>
</table>

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

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

Voice and screen recordings can occupy a great deal of hard disk drive space on the Quality Management server that hosts the recording file storage location. To protect the recording file storage location from running out of the free space required for normal operations and to prevent crashes, the Quality Management halts recording when the available hard drive disk space fall below 2 GB. The recordings remain on the client machine until you free up disk space on the storage location.

**Supported Remote Agent Configurations**

Some companies allow their agents to work offsite. When installing Quality Management, you must ensure that you use a remote agent configuration that is supported by Quality Management.

**Software VPN Support for Server Recording**

Quality Management supports the following Server Recording (SPAN) configurations when using the Cisco Systems VPN client:

- A non-IP phone using Cisco Unified Mobile Agent for both voice and screen recording
For more information on Cisco Unified Mobile Agent, see the *Cisco Mobile Agent Data Sheet*. This document can be accessed at the following Cisco website:


**Hardware VPN Support for Network Recording**

Quality Management supports remote agents with a Network Recording and Monitoring capable IP phone or a Network Recording and Monitoring capable IP soft phone for both voice and screen recording using a Cisco 831 router or the Cisco 871 router.

**Software VPN Support for Desktop Recording**

Quality Management supports the following Desktop Recording configuration when using the Cisco System VPN client:

- Endpoint recording behind a VPN when using an IP soft phone

**Hardware VPN Support for Desktop Recording**

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

Quality Management 8.5 requires the following third-party applications in order to run successfully. These applications are not installed when you install Quality Management. They must be purchased and installed separately.

**Table 14. Required third-party applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>Installed Where</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2005 Standard Edition</td>
<td>Quality Management Database server or offboard server</td>
<td>Database</td>
</tr>
<tr>
<td>Service Pack 2 or Microsoft SQL Server 2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard Edition Service Pack 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Informix Client Software Development Kit 3.0.0</td>
<td>Quality Management Base Services server</td>
<td>Database</td>
</tr>
<tr>
<td>Adobe Reader 6.0 or later</td>
<td>Client machine</td>
<td>PDF-based reports and Quality Management user documentation. Free download at <a href="http://www.adobe.com">www.adobe.com</a></td>
</tr>
<tr>
<td>Java Runtime Environment (JRE) 1.6.0 update 13 or later&lt;sup&gt;a&lt;/sup&gt;</td>
<td>On the client machine where the Calabrio Screen Player Plugin is installed</td>
<td>Media playback for voice and screen from the Cisco Unified Workforce Optimization’s Search and Play widget and Evaluate and Review widget. Download from http://&lt;Base IP address&gt;:8088/TUP/QM/jre-6u13-windows-i586-p.exe, where &lt;Base IP address&gt; is the IP address for the Quality Management Base Services server.</td>
</tr>
<tr>
<td>Quality Management requires one of the</td>
<td>Client machine</td>
<td>Quality Management application widgets and HTML-based reports</td>
</tr>
<tr>
<td>following web browsers:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Firefox 3.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Microsoft Internet Explorer 7 or 8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>a</sup> The JRE is automatically installed when you install Quality Management Administrator. If you are using only the Cisco Unified Workforce Optimization, you must install the JRE on the client machine.
**Web Browser Considerations**

Our testing has found that the time required to fully render a page within the Cisco Unified Workforce Optimization can vary from one web browser family to the next. If user interface performance is a major concern to your business practice, the web browsers perform page rendering in the following order from fastest to slowest:

- FF 3.x or later
- IE 8
- IE 7

**Supported IP Phones**

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

**Supported IP Phones for Desktop Recording and Server Recording**

For a list of supported IP phones, see the Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide. You can access this document at the following Cisco website:


**NOTE:** The Cisco website is subject to change without notice. If the above address does not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.

**NOTE:** Not all of the phones listed in this document are compatible with Quality Management. Phones have to be qualified to work with Quality Management before you install Quality Management.

**Supported IP Phones for Network Recording**

For a list of phones that support Quality Management, see the Cisco Unified Communications Manager Features and Services Guide. You can access this document at the following Cisco website:


**NOTE:** The Cisco website is subject to change without notice. If the above address does not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document appears in the search results list.
NOTE: Not all of the phones listed in this document are compatible with Quality Management. Phones have to be qualified to work with Quality Management before you install Quality Management.

Cisco IP Communicator Considerations

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

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

Qualifying Phones for Quality Management

Some phones do not function with the Desktop Recording service (Endpoint). Verify your phones support endpoint monitoring (hard IP phones must have a PC port) before installing Quality Management. Server Recording (SPAN) for Unified CCX is not limited by this requirement.

Phones Tested for Desktop Recording and Server Recording

The following phones were tested and work with Quality Management when running Desktop Recording and Server Recording.

- 7910, 7940, 7941G, 7960, 7961G, 7970G — These phones have a PC port.
- Cisco IP Communicator 7.x

Phones Tested for Network Recording

The following phones were tested and work with Quality Management when running Network Recording.

- Cisco IP Communicator IP 7.x

Supported Cisco Unified Outbound Dialer Modes

Quality Management supports the Direct Preview dialing mode.
Recording Requirements

You can configure Quality Management to record an agent’s calls from the agent’s desktop or from a server. This section describes the requirements and consideration for the following scenarios:

• Using Desktop Recording service (Endpoint) to record from an agent’s desktop
• Using Server Recording (SPAN)
• Using Network Recording

**NOTE:** Shared lines are not supported for Server Recording, Desktop Recording, or Network Recording.

Required Codecs

The system environment determines which codecs that Quality Management supports.

**Required Codecs for Unified CCX**

Quality Management supports the G.711, G.722, and G.729 codecs with Desktop Recording (Endpoint), Server Recording (SPAN), and Network Recording. If you do not use a supported codec, expect the following results.

• The Desktop Recording service and Network Recording service will not function correctly if IP phones use any other codec.
• Unsupported codecs will result in a 1KB (8bytes) recording (raw file).

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

Server Recording (SPAN) and Network Recording Considerations

**General**

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

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

You need to configure which devices will be recorded using Server Recording or Network Recording. The VoIP Devices node in Quality Management Administrator enables you to search for the devices configured in Unified CM and enable the devices for Server Recording or Network Recording. You can then associate an agent, a Monitor
service server (Server Recording only), and a Network Recording server with those devices. See “VoIP Devices” in the Administrator User Guide for more information.

Server Recording and Network Recording have the following limitation:

- A device cannot be registered for Server Recording and Network Recording at the same time. You can, however, change the configuration from Server Recording to Network Recording. Or change a configuration from Network Recording to Server Recording.

**Server Recording (SPAN)**

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

For Server Recording, the Monitor service must be connected to the SPAN port on the switch that is connected to the phones you want to record. See Configuring and Troubleshooting VoIP Monitoring for more information on SPAN. This document can be accessed at the following Cisco website:


**NOTE:** The Cisco website is subject to change without notice. If the above address does not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document will appear in the search results list.

Server Recording acts as a backup to Desktop Recording (Endpoint). If a device configured for Server Recording is detected by the Desktop Recording service (Endpoint), then the Desktop Recording service will be used to capture the voice recording.

**NOTE:** If you want to use Server Recording exclusively, do not daisy chain a phone to your PC.

The daily folder for Server Recording is located on your C: drive.

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

**Network Recording**

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

For more information on this subject, see the “Monitoring and Recording” section of the Cisco Unified Communications Manager Features and Services Guide available at:


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

• To enable Network Recording for Quality Management, you must set up Unified CM for Automatic Recording on each line you want to record.

• If you select On Demand for each line you want to record, a third-party application is required to initiate the recording. Quality Management will only capture the voice and screen from the point where a request to record is issued. Quality Management does not initiate the recording. Quality Management does not capture the entire conversation.

• The only “backup” for Network Recording is a backup recording server running the Network Recording service and that is only when you shut down the primary recording server using Top Down scheduling in Cisco Unified CM. No additional configuration within Quality Management Administrator is required to make this work. The backup recording server begins recording calls when the primary recording server is not available. Not available could mean any of the following:
  – The Network Recording service on the primary recording server stopped
  – The primary recording server is shut down
  – The primary recording server is no longer connected to the network
  – The Network Recording service on the primary recording server reached capacity for simultaneous recordings

  **NOTE:** When the primary recording server shuts down or is no longer connected to the network, there will be a delay before recording starts on the backup recording server. You might miss a portion at the beginning of each recording until the primary recording server is online again.

• Workflow rules apply to all recorded calls. For example, if you configure a quality management workflow to save five recordings for a specific agent, and there are only two recordings, only the two recordings will be kept.
When setting up your phones for Network Recording, consider the following:

- Not all IP phones support Network Recording. Phones supported for Network Monitoring and Recording can be found in the *Cisco Unified Communications Manager Features and Services Guide* available at:


- A device cannot be configured for Server Recording and Network Recording at the same time. You can, however, change the configuration from Server Recording to Network Recording, or change a configuration from Network Recording to Server Recording.

- Unlike Server Recording, Network Recording does not act as a backup to Desktop Recording (Endpoint). If a device is configured in Quality Management Administrator for Network Recording, then Network Recording will be the only recording approach used for that device.

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

Network Recording supports the recording of Secure Real-time Transport Protocol (SRTP) calls with Cisco Unified CM 8.0 or later. See the Cisco Unified CM documentation for more information on configuring SRTP for Quality Management. This includes the configuration of a secure SIP trunk and certificate management. Use Site Configuration Setup for Quality Management to configure the certificate required by Cisco Unified CM to establish a trusted relationship for security key exchange.

The daily folder for Network Recording is located on your C: drive.

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

**Configuring Cisco Unified CM for Live Monitor**

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

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

- Live Monitor only works on phones that include a Built In Bridge (BIB). This includes IP Communicator 7.x or later.

- Use Live Monitoring instead of CAD Silent Monitoring with Network Recording when running Unified CCX 8.0(2) or earlier because CAD does not handle duplicate packets.
• All phones used for live monitoring must be set up for Network Recording in both Unified CM Administration and Quality Management Administrator.

• Phones used to monitor users do not need to be configured for Network Recording. The extension a supervisor or manager enters in the My Extension field in the Live Monitoring application must be added to Unified CM application user group that was configured for Call Monitoring (that is, the Java Telephony API (JTAPI) user) and have a calling search space for the extension that includes the user's line or device partition to allow monitoring the agent.

• Assign the Standard CTI Allow Call Monitoring group to the JTAPI user in Cisco Unified CM. Live Monitoring requires the permissions provided by this group.

• Live Monitor support for Secure calls and multiple codecs is defined by Unified CM. It is not enabled or restricted by Live Monitor.

• If a supervisor or manager is configured to be recorded using any recording method (for example, Desktop Recording, Server Recording, or Network Recording), any live monitoring sessions they conduct might be recorded. The calls will only be uploaded and displayed as calls in the Quality Management system if they match either an archive workflow or a quality management workflow. To avoid this behavior, a Quality Management administrator can configure a second extension in Quality Management Administrator, and possibly Unified CM, that is not configured to be recorded. Therefore, all calls on the first extension will be recorded, but live monitor sessions conducted on the second extension will not be recorded.

**Configuring Unified CM for Network Recording**

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

**TASK**

• Enable IP phone BIB (Built In Bridge) to allow monitoring and recording.

  *ADDITIONAL INFORMATION:* See “Cisco Unified IP Phone Configuration” in the *Cisco Unified Communications Manager Administration Guide* for more information.

• Add a user for the monitoring and recording application.

  *ADDITIONAL INFORMATION:* See “Application User Configuration” in the *Cisco Unified Communications Manager Administration Guide* for more information.

• Add the use to a user group that allows monitoring and recording.

  *ADDITIONAL INFORMATION:* See “Application User Configuration” and “User Group Configuration” in the *Cisco Unified Communications Manager Administration Guide* for more information.

• Configure tones for monitoring and recording.
ADDITIONAL INFORMATION: See “Service Parameters Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Configure DN for a monitoring calling search space.

ADDITIONAL INFORMATION: See “Directory Number Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Enable recording for a line appearance.

ADDITIONAL INFORMATION: See “Directory Number Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Create a recording profile.

ADDITIONAL INFORMATION: See “Recording Profile Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Create a SIP trunk that points to the recorder.

ADDITIONAL INFORMATION: See “Trunk Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Create a route pattern for the recorder.

ADDITIONAL INFORMATION: See “Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

- Configure the recorder for redundancy.

ADDITIONAL INFORMATION: See “Trunk Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

Desktop Recording Service (Endpoint) Requirements

This section contains information about requirements for using the Desktop Recording (Endpoint) service.

**Enabling Required Phone Device Parameters**

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

**TASK**

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

**STEP RESULT:** The phone device’s Phone Configuration page appears.
2. In the Product Specific Configuration Layout section, set these parameters to Enabled:

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

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

3. Click Update.

**Hard Disk Drive Space on Agent’s Computers**

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

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

After the space is freed up, recordings will resume.

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

**Network Interface Cards**

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

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

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

If the workaround does not solve the problem, the VLAN ID of the IP phone to which the agent computer is directly connected must be added to the VLANs tab of the Intel NIC’s Network Connection Properties dialog box.
The IP phone’s VLAN ID can be obtained from the phone’s Network Configuration screen (press Settings and then choose Network Configuration). For more information, see the documentation specific to your version of the Unified CM and IP phone model.

The following is a partial list of supported NICs:

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

**Phone Configurations for the Desktop Recording Service**

Two phone configurations for endpoint recording are supported:

- Hard IP phone and agent computer daisy-chained to the network (Figure 3). The only time you should daisy-chain your phones is when you intend to use endpoint recording.

  **NOTE:** Multiple daisy-chained phones are not supported.

**Figure 3.** Hardware setup (hard IP phone) for the Desktop Recording service
• Cisco IP Communicator soft IP phone on the agent’s computer, connected to the network (Figure 4). No hard IP phone can be on the same network connection as the agent PC. Cisco IP Communicator must be in the computer’s startup menu so that it is detected by the Desktop Recording service.

**NOTE:** Information about configuring phones for server recording can be found in the document Configuring and Troubleshooting VoIP Monitoring. This document can be accessed at the following Cisco website:


**NOTE:** The Cisco website is subject to change without notice. If the address above does not work, go to the Cisco home page (www.cisco.com), enter the name of the document in the Search field, and click Go. The document will appear in the search results list.

![Figure 4. Hardware setup (Cisco Communicator soft IP phone) for the Desktop Recording service](image)

**Firewall Requirements**

For Quality Management to function correctly, the ports listed in this section must be opened in the Windows Firewall. If the Windows Firewall/Internet Connection Sharing (ICS) service is running when Quality Management is installed, the Quality Management installation process opens all ports and programs as needed except those for Microsoft SQL Server (by default, 1433 and 1434) and Informix Client SDK (by default, 1504). See “Microsoft SQL Server” on page 52 for information on adding Windows Firewall exclusions and allowing remote connections for Microsoft SQL Server and Informix Client SDK.

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

Table 15 lists the ports on the Base Services server that must be opened in the Windows Firewall.

Table 15. Port usage for the Base Services server

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>8088</td>
<td>TCP</td>
<td>Jetty service (Jetty port)</td>
</tr>
<tr>
<td>8448</td>
<td>TCP</td>
<td>Jetty service (Jetty SSL port)</td>
</tr>
<tr>
<td>59011</td>
<td>TCP</td>
<td>Sync service</td>
</tr>
<tr>
<td>59103</td>
<td>TCP</td>
<td>Data API servicea</td>
</tr>
</tbody>
</table>

a. The surrogate port is located on the Quality Management server. The Data API Service uses this port to communicate with the Surrogate.

CTI Services Server

Table 16 lists the ports on the CTI Services server that must be opened in the Windows Firewall.

Table 16. Port usage for CTI Services server

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>52102</td>
<td>TCP</td>
<td>CTI service</td>
</tr>
</tbody>
</table>
Database Services Server

Table 17 lists the ports on the Database Services server that must be opened in the Windows Firewall.

Table 17. Port usage for Database Services server

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>2303</td>
<td>UDP</td>
<td>DB Proxy service</td>
</tr>
<tr>
<td>52103</td>
<td>TCP</td>
<td>DB Proxy service</td>
</tr>
<tr>
<td>59100</td>
<td>TCP</td>
<td>Upload Controller service</td>
</tr>
<tr>
<td>PgSvc.exe</td>
<td>—</td>
<td>Screen recording service</td>
</tr>
<tr>
<td>59102</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>59500-60300</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>RecordServer.exe</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>sqlbrowser.exe</td>
<td>UDP</td>
<td>SQL Server Browser&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<sup>a</sup> If the database uses a named instance, sqlbrowser.exe needs to be running and added to the exception list in the firewall. If you are using the default instance (that is, the Instance Name field in QM Databases is empty), you do not need to add sqlbrowser.exe to the firewall exception list.
Quality Management Server for Server Recording and Network Recording Deployments

Table 18 lists the ports on the Quality Management server that must be opened in the Windows Firewall for Server Recording and Network Recording deployments.

Table 18. Port usage for Quality Management server

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>59102</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>59500-60300</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>RecordServer.exe</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>59101</td>
<td>TCP</td>
<td>Monitor service</td>
</tr>
</tbody>
</table>

Monitor Services Server for Server Recording Deployments Only

Table 19 lists the ports on the Monitoring Services server that must be opened in the Windows Firewall for Server Recording deployments.

Table 19. Port usage for Monitor Services server for Server Recording Deployments

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>59101</td>
<td>TCP</td>
<td>Monitor service</td>
</tr>
</tbody>
</table>
Network Recording Services Server for both Server Recording and Network Recording Deployments

Table 20 lists the ports on the Network Recording Services server that must be opened in the Windows Firewall for both Server Recording and Network Recording Deployments.

Table 20. Port usage for Network Recording Services server for both Server Recording and Network Recording Deployments

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>59102</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>59500-60300</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>RecordServer.exe</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>TCP</td>
<td>Network Recording service</td>
</tr>
<tr>
<td>5060</td>
<td>UDP</td>
<td>Network Recording service</td>
</tr>
</tbody>
</table>

Voice/Screen Services Server

Table 21 lists the ports on the Voice/Screen Services server that must be opened in the Windows Firewall.

Table 21. Port usage for Voice/Screen Services server

<table>
<thead>
<tr>
<th>Port/Program</th>
<th>Type</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>8088</td>
<td>TCP</td>
<td>Jetty service (Jetty port)</td>
</tr>
<tr>
<td>8448</td>
<td>TCP</td>
<td>Jetty service (Jetty SSL port)</td>
</tr>
</tbody>
</table>
Prerequisites

Before you install Quality Management, you must read this section and ensure all prerequisites are complete.

Pre-installation and Deployment Checklists

This document provides the following checklist to help the installation go smoothly.

- Pre-installation Checklist—Use this checklist to gather configuration information before you install Quality Management.
- Deployment Activities—Use these lists to plan what you need to do to install and deploy Quality Management.
- Installation Checklist—Use this checklist in conjunction with the information in this chapter when installing Quality Management and running the Site Configuration Setup tool.

See “Checklists and Activities” on page 159 for details.

Microsoft Server 2008

If you are installing Monitoring and Recording Services on Windows Server 2008, you must enable Desktop Experience. Desktop Experience allows the end users to export screen recordings or WMA from the Calabrio One interface.

Enabling Desktop Experience on Windows Server 2008

**TASK**

1. From the server running Windows Server 2008, choose Start > Server Manager.

2. Click Features, and then click Add Features.

**STEP RESULT:** The Add Features Wizard appears.

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

4. Reboot the server.
Microsoft SQL Server

Before you install the Quality Management, you must install Microsoft SQL Server 2005 or Microsoft SQL Server 2008, either co-resident with the Quality Management Database server or on an off-board server, and configure it for Quality Management.

Installing Microsoft SQL Server

Install Microsoft SQL Server per the SQL Server documentation.

When installing the SQL Server, use the following settings:

- Only select the SQL Server Database Services component from the Components to Install screen.
- Only select Management Tools from the Feature Selection screen. To access this screen, click Advanced on the Components to Install screen.
- Only select Management Tools from the Feature Selection screen. To access this screen, click Advanced on the Components to Install screen.
- Select the Mixed Mode option in the Authentication Mode screen.
• When configuring the SQL Server instance, select the following option under SQL Collations in the Collation Settings dialog box (Figure 5):

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

This option is required to assign the Latin1_General_CP1_CI_AS property to Server Collation in the Server Properties window (Figure 6). See http://msdn.microsoft.com/en-us/library/ms180175.aspx for more information.

Figure 5. Collation Settings dialog box
Prerequisites
Microsoft SQL Server

Figure 6. Server Properties dialog box

The SQL Server installation installs the SQL Browser Service. By default, this service is set to be started manually, not automatically.

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

Creating an SQL Server User Login for Initial Installation

Create a user login for the SQL server to use when you initially install Quality Management. The Site Configuration Setup tool requires the dbcreator role for this user login when creating the Quality Management database.

The following task assumes you are creating a user login responsible for the initial installation of Quality Management.

TASK
1. On the SQL Server computer, start SQL Server Management Studio.
2. From the navigation tree in the left pane, select Security > Logins under the SQL Server instance name.
3. Right-click Logins and select New Login from the popup menu to display the Login - New dialog box.

4. On the General page, enter a name for the new login, select the authentication mode SQL Server Authentication, enter a password, clear the Enforce password policy check box, and choose English as the default language.

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

5. On the User Mapping page, select SQMDB from the list of Users mapped to this login, and then click OK.

6. On the Server Roles page, select the dbcreator check box from the list of server roles, and then click OK.

**STEP RESULT:** The new login user appears in the list in the right pane.

### Configuring Microsoft SQL Server for Quality Management


### Microsoft SQL Server 2008 Requirements

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

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

### Adding Firewall Exclusions by Application

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

**TASK**

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

**STEP RESULT:** The Windows Firewall application starts.
2. On the Exceptions tab, click Add Program.

**STEP RESULT:** The Add a Program dialog box appears, listing all applications on the server.

3. Click Browse and navigate to the SQL Server engine at C:\Program Files\Microsoft SQL Server\MSQL.1\Binn\sqlservr.exe.

**ADDITIONAL INFORMATION:** If there are more than one instance, “MSQL.1” might not be the correct instance. Verify that MSQL.1 is the correct instance before adding a Windows Firewall exclusion.

4. Click OK.

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

**STEP RESULT:** All ports that SQL Server 2005 or SQL Server 2008 opens are now accessible.

### Allowing Remote Connections

Microsoft SQL Server 2005 disables remote connections by default. (This is enabled by default in Microsoft SQL 2008.) Microsoft SQL Server 2005 only allows connections from the same server by default. Quality Management requires remote connections for Quality Management Administrator, Site Configuration Setup, Reporting, and Quality Management Monitoring and Notification Service. Use the following task to enable remote connections in Microsoft SQL Server 2005.

**TASK**


2. Under Configure Surface Area for localhost, click Service Area Configuration for Services and Connections.

3. Select the View by Instance tab, and then expand the tree for the instance configured for Quality Management. Click Remote Connections.

4. From the options on the resulting window, select:

   - Local and remote connections
   - Using TCP/IP only

**NOTE:** All other options should be clear.
5. Click OK.

**STEP RESULT:** Microsoft SQL Server 2005 now allows remote connections.

**Configuring the SQL Server Browser**

The SQL Server Browser, an SQL Server component, allows a client to search for named instances. By default, the service status for this component is Stopped and the service startup type is Manual. Use this task to start the SQL Server Browser service if you are using a named instance (instead of the default instance). If you are using a default instance you can skip this task.

**TASK**


**STEP RESULT:** The Windows Services utility starts.

2. In the list of services, locate SQL Server Browser.

3. Right-click the name and choose Properties.

4. In the Properties dialog box, change the startup type from Manual to Automatic.

5. Click Start to start the service, and then click OK.

**STEP RESULT:** SQL Server Browser starts automatically.

**Microsoft SQL Roles**

If necessary, create several user logins for the SQL server. For example, you can configure one user login responsible for installation and upgrades and another user login responsible for day-to-day database activities. Assign the following roles to a user login responsible for installation and upgrades:

- **db_datareader**—Allows the user to read the database.
- **db_datawriter**—Allows the user to write to the database.
- **db_owner**— Allows the user to change the schema of the database. This role is only required during installation and upgrades.
- **dbcreator**—Required when the Site Configuration Setup creates the SQMDB database automatically. If you assign the dbcreator to the user login, and Site Configuration Setup creates the SQMDB database, the user login is the dbowner of the SQMDB database.
Creating an SQL Server User Login for Initial Installation

Create a user login for the SQL server to use when you initially install Quality Management. The Site Configuration Setup tool requires the dbcreator role for this user login when creating the Quality Management database.

The following task assumes you are creating a user login responsible for the initial installation of Quality Management.

**TASK**

1. On the SQL Server computer, start SQL Server Management Studio.

2. From the navigation tree in the left pane, select Security > Logins under the SQL Server instance name.

3. Right-click Logins and select New Login from the popup menu to display the Login - New dialog box.

4. On the General page, enter a name for the new login, select the authentication mode SQL Server Authentication, enter a password, clear the Enforce password policy check box, and choose English as the default language.

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

5. On the User Mapping page, select SQMDB from the list of Users mapped to this login, and then click OK.

6. On the Server Roles page, select the dbcreator check box from the list of server roles, and then click OK.

**STEP RESULT:** The new login user appears in the list in the right pane.

Creating an SQL Server User Login for Upgrades

Create a user login for the SQL server to use when you upgrade the Quality Management.

The following task assumes you are creating a user login responsible for installation and upgrades.

**TASK**

1. On the SQL Server computer, start SQL Server Management Studio.
2. From the navigation tree in the left pane, select Security > Logins under the SQL Server instance name.

3. Right-click Logins and select New Login from the popup menu to display the Login - New dialog box.

4. On the General page, enter a name for the new login, select the authentication mode SQL Server Authentication, enter a password, clear the Enforce password policy check box, and choose English as the default language.

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

5. On the User Mapping page, select SQMDB from the list of Users mapped to this login, and select the following check boxes from the Database role membership, and then click OK.

   - db_datareader
   - db_datawriter
   - db_owner

   **NOTE:** If you are upgrading from SQL Server 2000 to SQL Server 2005 Standard Edition or SQL Server 2008 Standard Edition on an existing Quality Management system, select the db_datareader and db_datawriter server roles.

   **STEP RESULT:** The new login user appears in the list in the right pane.

---

**Windows SNMP Services**

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

You can configure SNMP for notification in the Site Configuration Setup or under Site Configuration in Quality Management Administrator, in the Monitoring and Notification window.

SNMP allows you to monitor and manage a network from a single workstation or several workstations, called SNMP managers. SNMP is actually a family of specifications that provide a means for collecting network management data from the devices that reside in a network. SNMP also provides a method for those devices to report any problems that they are experiencing to the management station.
For more information on using this tool, see Microsoft SNMP documentation.

Installing Windows SNMP Services

This optional task describes how to install Windows SNMP services.

**Task**

1. On the Quality Management server, select Start > Control Panel and launch the Add or Remove Programs utility.
2. On the left of the Add or Remove Programs window, click Add/Remove Windows Components.
3. From the list of components, select Quality Management Tools, and then click Details.
4. From the list of available components, choose Simple Network Management Protocol and then click OK.

**Step Result:** The system prompts you for the Windows 2003 CD.

5. Insert the Windows 2003 CD in the drive and follow the instructions in the installation wizard to install SNMP.

JTAPI User

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

To add a JTAPI user for Unified CM, see the “Adding a New User” section in the Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager. The document is available at the following website:


**NOTE:** The Cisco website is subject to change without notice. If above address does not work, go to the Cisco home page (www.cisco.com), type the name of the document in the Search field, and click Go. The document appears in the search results list.
When you configure the JTAPI user, consider the following guidelines.

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

Active Directory

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

Use Active Directory with Quality Management to:

- Allow Quality Management users to use their existing Windows user name and password to access Quality Management. Using the Windows user name and password eliminates the problem of remembering and maintaining a separate user name and password.
- Enforce password security policies (for example, complexity level or duration), in a single instance across one or more domains.

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

Active Directory Configuration Guidelines

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

- The Quality Management server must be:
  - On the same domain as the end users who log in to Cisco Unified Workforce Optimization, or
  - On a trusted domain to the domain that contains the end users who log in to Cisco Unified Workforce Optimization
- There must be at least one configured domain.
- Each domain must have at least one configured user path
Active Directory Information

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

- Base DN
- Domain name
- Active Directory host name
- Active Directory IP address
- Port
- Active Directory display name, password, and user search base
- User records

Locating the Active Directory Domain Name

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

**TASK**

1. Log into the machine running Active Directory.


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

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

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

4. Note the domain name.

**ADDITIONAL INFORMATION:** The Site Configuration Setup tool requires the domain name for Active Directory.
Installing Quality Management

This chapter describes how to install Quality Management 8.5. When you install Quality Management 8.5, you must install the components in the following order.

1. Install the services for Quality Management.
2. Run Site Configuration Setup on the Quality Management server.
3. Install Quality Management client applications.

Services for Quality Management

Install the services for Quality Management according to the supported system configuration illustrated in Figure 1 on page 18.

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

IMPORTANT: Any time Site Configuration Setup starts after an installation or an upgrade, you must run it to completion in order for the system to function.

Installing Services

Use this task to install one or more services for Quality Management on a server.

TASK
1. Load the installation DVD in the server computer, and then navigate to the DVD in My Computer or Windows Explorer.
2. Double-click the file setup_MonRec_85<number>.exe to start the installation wizard.
3. Click Next.

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

3. Click Next.
**STEP RESULT:** The Custom Setup dialog box appears (Figure 7).

![Custom Setup window](image)

**Figure 7.** Custom Setup window

4. Select the first four services shown in the dialog. These services will be installed on the server.

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

**NOTE:** Select the Network Recording service and Monitor service only if you are using Server Recording or Network Recording.

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

5. Click Next, and then click Install.

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

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

Leave the window open. It will close on its own.

6. Click Finish to complete the installation of services.
**STEP RESULT:** The services you selected are installed, and Site Configuration Setup starts.

**AFTER COMPLETING THIS TASK:**

Complete the Site Configuration Setup windows. For more information, see “Running Site Configuration Setup” on page 73.

### Supporting Asian Languages

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

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

### Installing Supplemental Language Support

**TASK**

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

   **STEP RESULT:** The Control Panel window appears.

2. Double-click Regional and Language Options.

   **STEP RESULT:** The Regional and Languages Options window appears.

3. Click the Languages tab.

4. Select the Install files for East Asian languages check box.

   **STEP RESULT:** The Install Supplemental Language Support dialog box appears.

5. Click OK to dismiss the dialog box, and then click Apply.
6. Follow the prompts to install the fonts.

7. Restart the Quality Management Base Services server.

**ADDITIONAL INFORMATION:** The server might automatically restart after installing the fonts.

8. From Control Panel, double-click Fonts.

**STEP RESULT:** The Fonts window appears.

9. Select and copy the font you just added.

   - `batang.tcc` (Russian and Korean)
   - `mingliou.tcc` (Chinese and Japanese)

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

11. Restart the Quality Management Jetty service.

---

### Installing Client Applications for Quality Management

You can install the client applications from web pages that reside on the Quality Management Base Services server. Quality Management creates these web pages when you install the Base Services.

The web pages are:

- **Administrator.htm**—This page contains links to the install files for all three desktop applications—Quality Management Administrator, Calabrio Screen Player Plug-in, and the Desktop Recording service.

- **Desktop.htm**—This page contains a link to the Calabrio Screen Player Plug-in install files.

- **Recording.htm**—This page contains a link to the Desktop Recording service install files.

**NOTE:** If you install the Desktop Recording service on a desktop that also runs the CAD client, and the CAD installation includes a CAD Monitoring Server separate from the Unified CCX server, make sure that the PC running the Desktop Recording service can resolve the name of the CAD Monitoring Server. If the PC cannot resolve the name of the CAD...
Monitoring Server, recordings might be garbled when a CAD supervisor monitors a call.

**NOTE:** Install the client applications after you install the services for Quality Management.

### Enabling the Elevated Privileges Policy for Window Installer Installation

To allow users with limited privileges to install a client application for Quality Management on their computer (for example, an evaluator installing his or her own instance of Calabrio Screen Player Plug-in) you must enable the Windows policy “Always Install with Elevated Privileges” for both the User Configuration and the Computer Configuration.

By default, Windows Installer installations run in the context of the logged-on user. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the install to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

**Enabling the Windows Elevated Privileges Policy**

Use this task to elevate the privileges on a user’s computer so the user can install the client applications for Quality Management.

**TASK**

2. Right-click the appropriate organizational unit (OU) and from select Properties from the popup menu.
3. On the Group Policy tab, select the Group Policy Object (GPO) and then click Edit.
5. Double-click Always install with elevated privileges.
6. Set to Enabled, and then click OK.
8. Double-click Always install with elevated privileges.
9. Set to Enabled, and then click OK.
Installing Client Applications for Quality Management

Use this task to install client applications for Quality Management.

**Task**

1. From the computer where you want to install the desktop application, start Internet Explorer.

2. Enter the appropriate installation web page address in the Address field:

   - http://<base services IP address>:8088/TUP/QM/Administrator.htm
   - http://<base services IP address>:8088/TUP/QM/Desktop.htm
   - http://<base services IP address>:8088/TUP/QM/Recording.htm

**Step Result:** The installation web page appears.

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

Calabrio Screen Player Plug-in Limitations

If you install the Calabrio Screen Player Plug-in on a client machine running either the Vista or Windows 7 operating system where CAD is also installed, there is a conflict with the Next Generation Java Plug-in. By default, the Next Generation Java Plug-in is enabled. CAD requires the Next Generation Java Plug-in to be disabled so that you can use CAD’s keystroke macros. The Calabrio Screen Player Plug-in requires the Next Generation Java Plug-in to be enabled so that you can play screen recordings in Cisco Unified Workforce Optimization. You have to choose which feature you want to use on the client desktop and enable or disable the Next Generation Java Plug-in accordingly.

Enabling the Next Generation Java Plug-in

Use this procedure to enable Generation Java Plug-in so that you can play screen recordings in Cisco Unified Workforce Optimization.

**Task**

1. From the client desktop, choose Start > Control Panel.

**Step Result:** The Control Panel window appears.
2. Double-click Java Control Panel.

**STEP RESULT:** The Java Control Panel window appears.

3. Click the Advanced tab and scroll to Java Plug-in.

4. Select the Enable the next-generation Java Plug-in.

5. Click OK.

6. Restart your web browser.

**ADDITIONAL INFORMATION:** If you have more than one web browser open, you must restart all web browsers.

**Using Automated Package Distribution Tools**

MSI-based desktop application installations for Quality Management can be deployed (“pushed”) via automated package distribution tools that make use of the Microsoft Windows Installer service.

**Requirements**

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

**Execution**

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

**Per-Machine vs. Per User**

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

**Privileges**

Quality Management installations require either administrative or elevated privileges.

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

If the installation is run in the context of an administrative account, there is no need to enable policies to grant elevated privileges.
If the installation is run in the context of an account with reduced privileges, then it must be deployed with elevated privileges. The target machine must have the Windows policy “Always Install with Elevated Privileges” enabled for both the User Configuration and the Computer Configuration. When this policy is enabled, Windows Installer installations will run in a context with elevated privileges, thus allowing the installation to successfully complete complex tasks that require a privilege level beyond that of the logged-on user.

**Automated Package Installation vs. Manual Installation**

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

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

```
<user-defined path>\WFO_QM\Jetty\webapps\TUP\QM
```

You can also generate MSI packages for Quality Management using the ConfigureMsi.exe utility and unconfigured installation templates, available on the Quality Management installation DVD.

Quality Management does not support alteration of these files or the use of other MSI files included with the product at other locations.

The requirements for supported operating systems, product deployment configurations, installation order, and server/client version synchronization for automated package installation is the same as manual installation. Quality Management does not support altering the supplied MSI packages to circumvent the installation criteria.

**Multiple Software Releases**

Do not combine multiple software releases into a single deployment package. You must distribute each Quality Management software release in its entirety as a distinct deployment. Quality Management does not support combining multiple releases (for example, a software package’s base release and a subsequent service release) into a single deployment package.

**Reboots**

Any reboots associated with Quality Management installations are required. If you suppress the installation’s default reboot behavior, you must reboot the target machine before running the installed applications to ensure expected functionality.

You can delay a reboot without any issues at this time, as long as a reboot occurs before you launch the installed applications. If it is determined in the future that delaying a reboot via command line suppression affects expected behavior, then that delayed reboot will not be supported.
Best Practices

Best practices recommendations are listed below.

**Windows Installer Logging**

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

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

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

This ensures that any loggable issues are captured efficiently.

**Deployment**

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

**Installation and Uninstallation Deployment Packages**

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

**Recommended Deployment Preparation Model**

Use the following deployment preparation model to test the deployment in a test environment before you deploy an update on your production server.

1. Use a lab environment to model the pending deployment.
2. Install the servers to obtain valid client installation packages.
3. Manually deploy client installation packages to ensure that the installs are compatible with your environment.
   This will isolate product installation vs. automated deployment issues.
4. Create your deployment packages in accordance with the requirements listed in “Requirements” on page 69.
5. Test the deployment packages.
6. At deployment time modify your deployment packages, replacing the client installation packages from the lab environment with valid client installation packages from the production server.
Client Installation Packages on the Installation DVD

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

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

- Clients
  - Admin
  - MediaPlayer
  - Recording

Configuring Client Installation Files

Use this task to configure client installation files with the ConfigureMsi tool.

**TASK**

1. Copy the Clients folder and all its contents from the Quality Management installation DVD to a PC that does not have the Quality Management Base services installed on it.

2. On the desktop, open a command window and navigate to the Clients folder.

3. Type ConfigureMsi.exe and press Enter.

   **STEP RESULT:** The configuration tool starts.

4. Type the IP address of the Base Host or Surrogate Host and press Enter.

5. Type the IP address of Surrogate Host 1 and press Enter.

6. Type the IP address of Surrogate Host 2 or none, if Surrogate Host 2 does not exist, and press Enter.

   **STEP RESULT:** The utility creates installation files for all Quality Management client applications.

**NOTE:** You can combine the base release and service releases of the same version of software into a single folder structure. The configuration tool detects and configure both types of install packages.
Running Site Configuration Setup

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

**NOTE:** You must run Site Configuration Setup on the computer that hosts the Quality Management server.

Site Configuration Setup launches automatically in Initial Mode after you install Quality Management. When Site Configuration Setup runs in Initial Mode, you cannot skip screens or jump around in Site Configuration Setup. Popup dialogs may prompt you for additional information when running in Initial Mode. These popup dialogs provide additional tasks or tools you must run to fully configure the system. Initial Mode disables the Tools menu. Any time you launch Site Configuration Setup thereafter, the Site Configuration Setup tool is in Update Mode. Update mode allows you to skip screens and jump around Site Configuration setup. Update Mode enables the Tools menu.

Site Configuration Setup does not display the same windows for each service installation, but only those relevant to that service. You can see different steps depending on your Quality Management configuration.

Site Configuration Setup performs the following functions:

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

Entering Configuration Data in Initial Mode

This task explains how to enter configuration data during Initial Mode. Quality Management automatically runs the Site Configuration Setup tool after you install the services for Quality Management on the Quality Management server.

Note the following:

- You cannot move forward until you enter all required information.
- You cannot skip a step.
• You can go backwards at any time to revisit a previous step.
• Site Configuration Setup saves the text that you entered when you click Next.

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

**TASK**

1. Site Configuration Setup starts automatically after you install the services for Quality Management.

   **STEP RESULT:** When Quality Management Configuration Setup starts, the Quality Management Configuration Setup dialog box appears.

2. Enter the IP address of Quality Management Base server.

   **ADDITIONAL INFORMATION:** The Quality Management Base server is the computer where you installed the Base Services, Database Services, Voice/Screen Services, and Recording CTI Services.

3. Choose one of the following options:

   - If you are running Site Configuration Setup on the Quality Management Base Services server, choose the IP address of the Quality Management Base Services server from the IP Address for local Services drop-down list, and then click OK.
   - If you are running Site Configuration Setup on a different server, choose the IP address for the server from the IP Address for local Services drop-down list, and then click OK.

   **ADDITIONAL INFORMATION:** For example, if you want to run Network Recording on a different server and installed the Network Recording service and Monitor service on the server, choose the IP address for the Network Recording server from the IP Address for local Services drop-down list. If the computer has multiple NICs, multiple addresses appear in the IP Address for local Services drop-down list. Choose the IP address used for network traffic.

   **STEP RESULT:** The Installation Type dialog box appears (Figure 8).

**Figure 8. Installation Type dialog box**
4. Choose one of the following options and click OK.

- New Installation—Choose this option if this is a new installation.
- 2.X Upgrade—Choose this option if you are upgrading from QM 2.x.
- 8.X Upgrade—Choose this option if you are upgrading from Quality Management 8.x.

**STEP RESULT:** The Quality Management Database window in the Site Configuration Setup tool appears.

5. Complete the fields in Quality Management Database window and click Next.

**STEP RESULT:** If you are updating Quality Management from an earlier version, one of the following dialog boxes appears.

- Backup Files Found—This dialog box appears if backup files are found in the default location. Click Yes to use the QM LDAP backup files or click No if you do not want to use the existing backup files, and then click OK. If you choose No, your database will be empty.
- Backup Files Not Found—This dialog box appears if no backup files are found in the default location. Click Yes to choose a location for the QM LDAP Backup files or click No to save the QM LDAP backup files to C:\Program Files\Common Files\SQM\Backup\ldap folder, and then click OK.

The Database Exist dialog box appears. Click OK to upgrade your database.

The program upgrades the database and loads default data into the database. When finished, the Database Loaded Successfully confirmation box appears.

6. Click OK to dismiss the Databases Loaded Successfully confirmation box.

**STEP RESULT:** When finished, the Services Started Successfully confirmation box appears.

**NOTE:** This step might take several minutes to complete. The Services Started Successfully dialog box indicates the services started with no errors, but they might not be fully initialized and listening for requests when the message appears. Initialization continues after the message appears.

7. Click OK to dismiss the Services Started Successfully confirmation box.

**STEP RESULT:** The Cisco Unified CC Database window appears.

8. Complete the fields and click Next.

**STEP RESULT:** The Cisco Unified CM window appears.
9. Complete the fields and click Next.

*STEP RESULT:* The Quality Management CTI Service window appears.

10. Complete the fields and click Next.

*STEP RESULT:* The Active Directory Options dialog box appears.

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

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

*STEP RESULT:* The program installs the Cisco JTAPI Client. When finished, the JTAPI Configured Successfully confirmation box appears.

**NOTE:** If the Cisco JTAPI Client does not install correctly, you need to install JTAPI manually. See “Manually Installing the Cisco JTAPI Client” on page 80 for instructions.

12. Click OK to dismiss the confirmation box.

*STEP RESULT:* The Change Administrator Password dialog box appears (Figure 9).

![Change Administrator Password dialog box](image)

13. Enter a password for the Quality Management Administrator in the New password field, and enter it again in the Confirm new password field.

**ADDITIONAL INFORMATION:** Quality Management Administrator requires a password. The password must be between 1 and 32 characters long. It is case sensitive.

**NOTE:** If you are installing Quality Management for the first time, the Old password field is disabled.
14. Click OK to dismiss the dialog box.

**STEP RESULT:** The Enterprise Settings window appears.

15. Complete the fields and click Next.

**STEP RESULT:** The program validates the licenses. When finished, the License Validated Successfully confirmation box appears.

16. Click OK to dismiss the License Validated Successfully confirmation box.

**STEP RESULT:** The Recording File Storage Location dialog box appears.

17. Complete the fields and click OK.

**ADDITIONAL INFORMATION:** If you are installing Quality Management on Windows Server 2008, you must choose External Storage location, enter the path to the storage location, and then enter username and password in the Logon User pane.

**STEP RESULT:** The program initializes the Media server and installs PROXY Pro Gateway. When finished, the Media Server Settings dialog box appears with instructions on what to do next. The following steps explain these instructions.

18. Click OK to dismiss the Media Server Settings dialog box.

**STEP RESULT:** The PROXY Pro Gateway Administrator window appears.

19. In the navigation tree, select the Gateway Security node, and from the right pane, click the link “Click here to change Operation Security.”
STEP RESULT: The Gateway Security dialog box appears (Figure 10).

Figure 10. Gateway Security dialog box

20. On the Operation Security tab, enable permissions for administrators as follows:

- On the server that hosts the Network Recording service, select the Allow check box for Record to File.
- On the server that hosts the QM Voice and Screen services, select the Allow check box for Connect to File

21. Click OK.

22. If you are configuring Quality Management for Server Recording (SPAN), perform the following steps:

ADDITIONAL INFORMATION: If you plan to use Desktop Recording (Endpoint) or Network Recording, skip to step 23.

a. In the navigation tree, select General Settings.
Running Site Configuration Setup
Entering Configuration Data in Initial Mode

RESULT: A list of settings appears in the right pane.

b. Double-click Automatically move newly discovered workstations from "Unmanaged Hosts" to "All Hosts" group.

RESULT: The General Settings Properties dialog box appears.

c. From the General tab, select the "Automatically move newly discovered workstations from "Unmanaged Hosts" to the "All Hosts" group check box.

d. Click the Recording tab and select the Prefer user mode, and use this profile option.

e. Click Configure.

RESULT: The User Mode Profile Properties dialog box appears.

f. Choose [Custom] from the Choose Profile drop-down list.

g. Choose JPEG from the Image Type drop-down list.

h. Change Image Quality to 85%.

i. Change Capture Rate to 8.

j. Change Foreground to 4.

k. Change Background to 1.

l. Change Bandwidth Limit to 30 KB/sec.

m. Click OK. to save your changes.

RESULT: The User Mode Profile Properties dialog box closes.

n. Click OK to save your changes on the General Settings Dialog box.

RESULT: The General Settings Properties dialog box closes.

23. Close the PROXY Pro Gateway Administrator window.

24. Click Next.

STEP RESULT: The Upload Settings Window appears.

25. Complete the fields and click Next.

STEP RESULT: The Monitoring and Notification window appears.

26. Complete the fields and click Next.

STEP RESULT: The RTP Filters window appears.

27. Complete the fields and click Next.

STEP RESULT: The program generates client information and finishes the Site Configuration Setup. The Installation Complete confirmation box appears.
28. Click OK to dismiss the confirmation box.

**STEP RESULT:** A Start Services dialog box appears.

29. Click Yes.

**STEP RESULT:** The programs starts the services for Quality Management. When finished, the Services Started Successfully confirmation box appears.

30. Click OK to dismiss the confirmation box.

**STEP RESULT:** The Status window appears. This step shows the version of all installed Quality Management components.

31. Click Finish to close Site Configuration Setup.

**STEP RESULT:** The Site Configuration Setup closes.

**Manually Installing the Cisco JTAPI Client**

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

**TASK**

1. Stop the Quality Management CTI service.

2. Download the Cisco JTAPI Client from the Unified CM Plug-ins webpage.

3. Install the Cisco JTAPI Client on the Quality Management server.

4. Copy the jtapi.jar file from the C:\WINDOWS\java\lib folder to the C:\Program Files\Cisco\WFO_QM\ext folder.

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

5. Start the Quality Management CTI service.

6. Start Site Configuration Setup from the executable PostInstall.exe in C:\Program Files\Cisco\WFO_QM\bin.

7. Choose Tools > Test CTI Service.
STEP RESULT: The CTI Service Ready dialog box appears and displays the following message:

The CTI Service test completed successfully.

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

Site Configuration Setup Steps

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

Quality Management Database

Use the Quality Management Database window to configure connection information for the SQL Server instance where Quality Management information is stored.

NOTE: You can only change the information in the Quality Management Database window on the Quality Management Site Configuration Setup (PostInstall.exe).

Figure 11 displays the Quality Management Database window.

Figure 11. Quality Management Database window
Table 22. Quality Management Database fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/IP Address</td>
<td>The host name or IP address of the Quality Management Database server (the server on which SQL Server is installed).</td>
</tr>
<tr>
<td>SQL Instance Name</td>
<td>The Quality Management SQL Server instance name. Leave blank if you want to use the default instance.</td>
</tr>
<tr>
<td>Username</td>
<td>The DB service uses this name to access the Quality Management database (see “Microsoft SQL Server” on page 52).</td>
</tr>
<tr>
<td>Password</td>
<td>The DB service uses this password to access the Quality Management database (see “Microsoft SQL Server” on page 52). NOTE: Quality Management encrypts and saves this password when you click the Next button.</td>
</tr>
</tbody>
</table>

Configuration Settings Used By Services

If you change the settings on the Quality Management Database window, Table 23 shows when your changes take effect.

Table 23. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data API Service</td>
<td>Restart the service.</td>
</tr>
<tr>
<td>DB Proxy Service</td>
<td>Restart the service.</td>
</tr>
<tr>
<td>Sync Service</td>
<td>No restart required. The next sync period (every 10 minutes) applies the configuration settings.</td>
</tr>
</tbody>
</table>

Cisco Unified CC Database

Use the Cisco Unified CC Database window to identify the location of the Cisco Unified Contact Center Express (Unified CCX) database and configure access to the Cisco Unified CCX database. Quality Management uses this information to sync agents and teams from Cisco Unified CCX.

You can only edit the information in this step if the Site Configuration Setup tool (PostInstall.exe) is running on the Quality Management Base Services server. When viewed in Quality Management Administrator, it is read-only.
NOTE: If you are upgrading or modifying Unified CCX, observe the rules provided in “Rules for Upgrading or Modifying the Unified CC Database in Update Mode” on page 127.

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

Figure 12 displays the Cisco Unified CC Database window.

**Figure 12.** Cisco Unified CC Database window

![Cisco Unified CC Database Window](image)

**Table 24.** Cisco Unified CC Database fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize users with ACD</td>
<td>Select this check box to synchronize ACD (Automatic Call Distributor) agents, teams, and supervisors with Quality Management and to enable the other fields in the window. By default, this check box is selected and indicates that an ACD is available. You must select this check box for Unified CCX. When selected, Quality Management connects to Unified CCX Administration and imports the license. Quality Management retrieves the license from Unified CCX Licensing.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Side A Server Name</td>
<td>The name of the Unified CCX server for the Side A (primary) Cisco Unified CC database. If the server name contains a hyphen (-), replace the hyphen with an underscore (_) when you enter the server name in this field. This ensures the correct configuration of the file name. Site Configuration Setup appends _uccx to the name that appears the next time you run Site Configuration Setup. <strong>NOTE:</strong> Do not remove _uccx from the name.</td>
</tr>
<tr>
<td>Side A IP Address</td>
<td>The IP address of the Unified CCX server for the Side A (primary) Cisco Unified CC database.</td>
</tr>
<tr>
<td>Side B Server Name</td>
<td>The name of the Unified CCX server for the Side B (secondary) redundant Cisco Unified CC database, if one exists. If the server name contains a hyphen (-), replace the hyphen with an underscore (_) when you enter the server name in this field. This ensures the correct configuration of the file name. Site Configuration Setup appends _uccx to the name that appears the next time you run Site Configuration Setup. <strong>NOTE:</strong> Do not remove _uccx from the name.</td>
</tr>
<tr>
<td>Side B IP Address</td>
<td>The IP address of the Unified CCX server for the Side B (secondary) redundant Cisco Unified CC database, if one exists.</td>
</tr>
<tr>
<td>DB Instance Name</td>
<td>The name of the Cisco Unified CCX database. The name is rdsaux01_uccx and the field is disabled by default.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the Cisco Unified CCX database. The port number is 1504 and the field is disabled by default.</td>
</tr>
<tr>
<td>User</td>
<td>Login ID used to access the Cisco Unified CC database. This user must have write permission to the database. The login ID is uccxworkforce and the field is disabled by default.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used by uccxworkforce to access the Cisco Unified CC database.</td>
</tr>
</tbody>
</table>
Configuration Settings Used By Services

If you change the settings on the Cisco Unified CC Database window, Table 25 shows when your changes take effect.

Table 25. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Service</td>
<td>No restart required. The next sync period applies the configuration settings. Sync applies any changes without restarting the Sync service. Best practice recommends, updating the settings in the Cisco Unified CC Database in the following order: 1. Stop the Sync service and the Upload Controller service. 2. Back up the SQMDB catalog 3. Change the configuration settings on the Cisco Unified CC Database window 4. Start the Sync service. 5. Verify the data by looking for mass deactivations. 6. Restart the Upload Controller service. Restarting the Upload Controller services adds new calls to the database.</td>
</tr>
</tbody>
</table>
Cisco Unified CM

Use the Cisco Unified CM window to configure the Cisco Unified CM cluster in your system. The Cisco Unified CM window also allows you to configure the SOAP AXL user and Unified CM (JTAPI) user used by the CTI service to log in to the Unified CM.

Figure 13 displays the Cisco Unified CM window.

A Unified CM cluster has one or more 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. You can specify a primary and backup CTI Manager.

**NOTE:** A Unified CM cluster requires at least one CTI Manager.

You can choose any Unified CM to be your primary and backup CTI Manager. If you have Unified CM subscribers, to select one of these as your primary CTI manager.

**NOTE:** You can configure any machine as the primary CTI Manager, but it is a good idea to avoid using the publisher, because it already has
the highest load. Using another server as the primary CTI Manager helps avoid decreasing Unified CM performance.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP AXL Access Username</td>
<td>The AXL (Administrative XML Layer) authentication username for this cluster. This is configured when you configure Unified CM. Quality Management Administrator uses this user when configuring VoIP Devices in Record Server Configuration.</td>
</tr>
<tr>
<td>SOAP AXL Access Password</td>
<td>The AXL authentication password. This is configured when you configure Unified CM.</td>
</tr>
<tr>
<td>JTAPI User Username</td>
<td>The JTAPI user name. This is the application user with which all phone devices used for recording are associated. The CTI service logs into the Unified CM with this user. The user name must be between 1 and 32 alphanumeric characters.</td>
</tr>
<tr>
<td>JTAPI User Password</td>
<td>The JTAPI user’s password. This must be between 1 and 32 alphanumeric characters.</td>
</tr>
<tr>
<td>Publisher and Subscribers</td>
<td>The host name or IP address of the publisher and subscriber (if any) Unified CMs. You can enter 1 publisher Unified CM, and up to 8 subscriber Unified CMs.</td>
</tr>
<tr>
<td>Host Name/IP Address</td>
<td><strong>NOTE:</strong> When using hostnames, verify the server can resolve the name of the publisher and subscribers. If the hostname cannot be resolved, the CTI service cannot log in.</td>
</tr>
<tr>
<td>Primary CTI Manager</td>
<td>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. In a typical configuration, the Primary CTI Manager is a subscriber, not a publisher.</td>
</tr>
<tr>
<td>Backup CTI Manager</td>
<td>Select this option if the Unified CM is the backup CTI Manager. There can be 1 or no backup CTI Manager.</td>
</tr>
</tbody>
</table>
Configuration Settings Used By Services

If you change the settings on the Cisco Unified CM window, Table 26 shows when your changes take effect.

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI Service</td>
<td>Restart the service</td>
</tr>
<tr>
<td>Quality Management Administrator (VoIP Devices)</td>
<td>Reload the VoIP Device window.</td>
</tr>
<tr>
<td>Network Recording Service</td>
<td>No restart required. The next polling period applies the configuration settings.</td>
</tr>
<tr>
<td>Desktop Recording service</td>
<td>Restart the service</td>
</tr>
</tbody>
</table>

Adding a Unified CM Cluster

This task describes how to add a Unified CM cluster from the Cisco Unified CM window.

**TASK**

1. Click Add New Cluster.

2. Complete the fields on the tab created for the new cluster, and then click Save.
Deleting a Unified CM Cluster

There must be at least one Unified CM cluster configured. Quality Management does not allow you to delete the last remaining cluster.

**TASK**
1. Select the tab for the Unified CM cluster you wish to delete.
2. Click Remove Current Cluster.

**STEP RESULT:** The Delete Current Cluster dialog box appears (Figure 14).

**Figure 14. Delete Current Cluster dialog box**

3. Click Yes to confirm that you want to delete the cluster.

**STEP RESULT:** Quality Management deletes the cluster and removes the cluster’s tab from the Cisco Unified CM window.
Quality Management CTI Service

Use the Quality Management CTI Service window to configure the location of the CTI service.

Figure 15 displays the Quality Management CTI Service window.

Figure 15. Quality Management CTI Service window

Table 27. Quality Management CTI Service fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>(Read only) The IP address of the primary CTI Manager for this Unified CM cluster to which the CTI service will connect for call events.</td>
</tr>
<tr>
<td>Primary CTI Service Host Name/IP Address</td>
<td>The host name or IP address of the primary CTI service.</td>
</tr>
<tr>
<td>Backup CTI Service Host Name/IP Address</td>
<td>The host name or IP address of the backup CTI service.</td>
</tr>
</tbody>
</table>
## Configuration Settings Used By Services

If you change the settings on the Quality Management CTI Service window, Table 28 shows when your changes take effect.

**Table 28. When services start using the changed configuration settings**

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI Service</td>
<td>Restart the service.</td>
</tr>
<tr>
<td>Quality Management Administrator (VoIP Devices)</td>
<td>Reload the VoIP Device window.</td>
</tr>
<tr>
<td>Network Recording service</td>
<td>Restart the service.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you add a backup CTI service from the Site Configuration Setup utility while in Update Mode, you must restart the Network Recording service.</td>
</tr>
<tr>
<td>Desktop Recording service</td>
<td>Restart the service.</td>
</tr>
</tbody>
</table>
Adding a Backup CTI Service

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

**TASK**

1. From the Site Configuration Setup tool on the base machine or Quality Management Administrator, choose Quality Management CTI Service.

**STEP RESULT:** The Quality Management CTI Service window (Figure 16).

**Figure 16.** Quality Management CTI Service window

2. Choose Host Name or IP Address for the Backup CTI Service, and enter the host name or IP address. Save your changes by clicking Save in Quality Management Administrator or Next in the Site Configuration Setup tool.

3. Load the installation DVD in the server computer for the backup CTI Service, and then navigate to the DVD in My Computer or Windows Explorer.

4. Double-click the file setup_MonRec_851.exe to start the installation wizard.

**STEP RESULT:** The Custom Setup dialog box appears.

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

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

6. Click Next, and then click Install.
STEP RESULT: The installation wizard installs the services you selected and starts the Site Configuration Setup tool.

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

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

AFTER COMPLETING THIS TASK:

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

Enterprise Settings

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

The Enterprise Settings window enables you to:

• Enable automated software updates for client computers
• Configure Active Directory domains (in an Active Directory system only)
• Configure session time-outs for Cisco Unified Workforce Optimization and Quality Management Administrator
• View license information and update software licenses, if you are not using an ACD, by importing a new software license file
• Configure the locale for your system if your version of Quality Management supports other languages in addition to English
Figure 17 displays the Enterprise Settings window.

**Figure 17.** Enterprise Settings window with Active Directory

![Enterprise Settings window with Active Directory](image)

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

**Configuration Settings Used By Services**

If you change the settings on the Enterprise Settings window, Table 29 shows when your changes take effect.

**Table 29.** When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Clients (Enable Updates change)</td>
<td>Restart the client application.</td>
</tr>
<tr>
<td>Quality Management Administrator (AD Authentication and Administrator session timeout change)</td>
<td>Log into Quality Management Administrator.</td>
</tr>
</tbody>
</table>
Software Updates

Use the Automated Update feature to update the following client applications: Quality Management Administrator and Desktop Recording service. When you enable the Automated Update feature, every time one of these client application starts, it checks the Quality Management services to determine if a newer version is available. If there is a newer version, the Automated Update feature automatically installs the update on the client desktop.

**NOTE:** If you apply a service release (SR) update to the system, the best practice is to disable the Automated Update feature first. After the SR update is installed, manually test an updated instance of the Desktop Recording service, Cisco Unified Workforce Optimization, and Quality Management 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 Quality Management Administrator or Cisco Unified Workforce Optimization 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 time-out).
- Allow a user to remain logged in indefinitely (default setting).

To configure the session timeout period for Cisco Unified Workforce Optimization and Quality Management Administrator, enter the desired number of minutes of inactivity before timeout occurs in the minutes field.

**NOTE:** When you change the Session Timeout value for Quality Management Administrator, you must restart Quality Management Administrator before the changes can take effect.

If a user accessed one or more applications in the Cisco Workforce Optimization, each application displays a Timeout Warning dialog box 30 seconds before the application actually times out. If the user does not respond to the Timeout Warning dialog box, the application closes.
dialog box and the application are closed and an alert is sent to the user stating that the application timed out and was closed.

When you are playing a contact recording, the session remains in an active state. Cisco Unified Workforce Optimization does not time out when you are playing a contact recording.

**License**

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

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

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

If you clear the Synchronize Users with ACD check box, you are running Quality Management without an ACD and can only import the Cisco CR license. The License section displays the active license type, the number of licensed users associated with the license you purchased, and the Import Software License link.

**NOTE:** If you initially run Quality Management without Unified CCX, and then decide to run Quality Management with Unified CCX, Unified CCX licensing will override any licenses previously associated with Quality Management.

You can use the License section to modify your license (for example, add a Cisco CR license, or update an expired Cisco CR license).

You can use the Import Software License link to update your Cisco CR license if:

- Your current Cisco CR license has already or will soon expire
- You want to change the maximum number of licensed Cisco CR users

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

**Importing a License File**

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

**TASK**

1. Click the Import Software License link.

   **STEP RESULT:** Your browser starts and displays the License Management web page (Figure 18).

   **Figure 18. License Management Webpage**

   ![License Management Webpage]

2. Click Browse and navigate to the folder where your updated Cisco CR license file is stored, and select the file.

3. Click Upload.

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

4. Close the browser window.

   **STEP RESULT:** The results depend on the reason why you import a license.

   - The Enterprise Settings window does not display the uploaded Cisco CR license. Click Next on the Enterprise Settings window to validate the Cisco CR license. A message appears indicating whether or not the license successfully uploaded.
Licensing Rules

The license type determines what Cisco Unified Workforce Optimization records. The license type does not determine what a user can view in Cisco Unified Workforce Optimization.

The following rules apply to licensing:

- The license determines the applications that the users see in Cisco Unified Workforce Optimization.
- The license determines what is recorded, not what is viewed, in Cisco Unified Workforce Optimization. For example, if Agents X and Y use an Advanced license, they can record their screens. If the supervisor for these agents only has a QM license, the supervisor can still view the screen recordings made by these agents.
- Because managers using a Cisco CR license only see the Search and Play widget, a manager with agents using the Advanced license should purchase at least a QM license to see those quality recordings.
- Because supervisors using a Cisco CR license only see the Search and Play widget, a supervisor can only export audio recordings when an administrator configures the supervisor for export in Quality Management Administrator.

Active Directory

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

- The Quality Management server (or database server in multiple server configuration) must be on the same domain or on a trusted domain to the domain that contains the end users who log in to Cisco Unified Workforce Optimization
- There must be at least one domain configured
- Each domain must have at least one user path configured

The connection information that you enter in the Domain Information dialog box is verified using the entered credentials, and the user paths are validated when you click OK in the Domain Information dialog box.
### Table 30. Domain Information fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base DN</strong></td>
<td>The location of all Active Directory users in the directory server tree. This field is autofilled with a sample format with variable names that you replace with the domain information. Maximum number of characters allowed = 1000. If your hostname has more than 3 parts, add additional DC=domain statements to the beginning of the Base DN field.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Defaults to the first part of the string entered in the Base DN field. In most cases this is the domain name, but in some cases you must edit the default.</td>
</tr>
<tr>
<td><strong>Host Name/IP Address</strong></td>
<td>The host name or IP address of the Active Directory server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port used to access the Active Directory server. The field is autofilled with the default port 389, or 636 if you are using SSL (Secure Socket Layer).</td>
</tr>
<tr>
<td><strong>NOTE:</strong> If you change the port to anything other than 389 or 636, clearing or selecting the Use SSL check box will not change the port.</td>
<td></td>
</tr>
<tr>
<td><strong>Display Name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>User Password</strong></td>
<td>The user’s password.</td>
</tr>
<tr>
<td><strong>User Search Base</strong></td>
<td>The node in the Active Directory directory under which the user resides. Maximum characters allowed = 1000.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this check box to use SSL for connection to Active Directory. The check box is clear by default and indicates SSL is not enabled. Clearing or selecting this check box changes the default port number in the Port field.</td>
</tr>
<tr>
<td><strong>Add Certificate</strong></td>
<td>Click this button to locate the Certificate Authority (CA) certificate for AD. AD with SSL requires this certificate. The certificate provides the AD identity and public key for SSL communication. Contact your AD administrator for the location of the CA certificate for AD. In many cases, the Certificate Authority on the AD machine issues the CA certificate for AD. If this is the case, you can access the certificate from: http://&lt;AD server IP address&gt;/certsrv Download the certificate from this website by clicking Download a CA certificate, Certificate Chain, or CRL and save it to a folder. Then click Add Certificate to import the certificate. <strong>NOTE:</strong> After you import the certificate and save your changes, log out of Quality Management Administrator and log back in to verify the certificate works.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View Certificate</td>
<td>Select this button to view the certificate associated with AD.</td>
</tr>
</tbody>
</table>
| User Records (OUs)    | One or more paths to user records (OUs). Click Add to add at least one path, or Remove to remove an existing path. Maximum characters allowed = 1000. You must specify Active Directory paths from the most specific to the least specific (from left to right in the path statement). For example, if the AD tree is:

```
ou=US
  ou=Minnesota
    ou=Minneapolis
      ou=Users
```

Then the user record appears as follows:

```
ou=Users,ou=Minneapolis,ou=Minnesota,ou=US
```

Quality Management will search subtrees by default. For example, you could write the user record path as follows, and Quality Management will search all the subtrees under Minnesota.

```
ou=Minnesota,ou=US
```
Adding an Active Directory Domain

This task describes how to add an Active Directory domain.

**TASK**

1. Click Add in the Active Directory section.

   **STEP RESULT:** The Domain Information window appears (Figure 19).

**Figure 19.** Domain Information dialog box

![Domain Information dialog box](image)

2. Complete the fields as described in “Active Directory” on page 98 and click OK.
Removing an Active Directory Domain

This task describes how to remove an Active Directory domain.

**TASK**
1. Select the Active Directory domain you want to delete from the list in the Active Directory section of the Enterprise Settings window.
2. Click Remove.

Locale

Use the Locale section to enable the language used in your contact center.

A site has only one locale. All agents, supervisors, evaluators, and managers must use the same locale. You cannot assign one locale to a set of agents and another locale to a different set of agents.

**Enabling a Locale**

The following task describes how to enable the locale for Quality Management.

**TASK**

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

**ADDITIONAL INFORMATION:** You can enable only one locale per Quality Management system.

Recording File Storage Location

Use the Recording File Storage Location step to change the location where recordings (screen or voice, depending on which server you are running the Site Configuration Setup tool) are stored on the server.
Figure 20 displays the Recording File Storage Location window.

![Recording File Storage Location window](image)

Table 31. Recording File Storage Location fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Recording</td>
<td>You can change the storage location to any local or external folder. You do not have to store recordings on the machine that hosts the Voice and Screen services.</td>
</tr>
<tr>
<td>Screen Recordings</td>
<td>(Advanced license only) You can change the storage location to any local or external folder. You do not have to store recordings on the machine that hosts the Voice and Screen services. Because the Voice and Screen services are on the same server, you can choose to use the same path used for the voice recordings. <strong>NOTE:</strong> The File Transfer Servlet that is part of the Voice and Screen services must run as a user who has access to the location you choose for recordings.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the machine that hosts the Voice and Screen services and the voice recordings, and the path where voice recordings are stored.</td>
</tr>
</tbody>
</table>
### Use Same Path as Voice Recordings
Select this check box to save screen recordings in the same folder as voice recordings.

### Local Storage Location
Choose this option to store the voice and screen recordings on the Quality Management server.

### External Storage Location
Choose this option to store the voice and screen recordings on an external server.

*note:* If you change the storage location from local to external storage in update mode, you must first uninstall the DB service on the server that hosts the Voice and Screen services (in Control Panel’s Add or Remove Programs, remove PROXY Pro Gateway). When you run the Set Recording Home Directory tool, the DB service is reinstalled automatically. See “Entering Configuration Data in Update Mode” on page 127 for additional information.

### Storage Location
The path where voice and screen recordings are stored. Click Browse and navigate to the storage folder.

### Username
If you selected an external storage location, enter the username required to access that location. If the user is a domain user, enter the name with the format `<domain>\<username>`.

For external screen storage and playback to work, you must provide a domain user that has read and write access to the local server and the external storage system.

This user must meet these requirements:

- The local server must know the user (the user is a trusted domain user).
- If the user is a domain user, the domain specified must be trusted by the local server. This means the Recording server that you are configuring has to be on a domain that trusts or is trusted by the domain you are entering.
- The user must be able to log on as a service.
- The user must have read/write access to both the external drive location entered AND the location where Quality Management is installed on the local server.

### Password
If you selected an external storage location, enter the password required to access that location.
Configuring the Recording Location

This task describes how to configure the storage recording location.

**TASK**


   **STEP RESULT:** The Recording File Storage Location window appears.

2. Select if you want to store recordings in a local or external storage location, and then enter the desired location in the IP Address and Storage Location fields.

3. If you selected an external location, enter the username and password required to access that location. If the user is a domain user, enter the name with the format `<domain>\<username>`.

4. Click OK.
Upload Settings

Use Upload Settings step to schedule uploading of peak and off-peak recordings from the agent desktops to the Voice and Screen servers, in addition to recording metadata to the Quality Management database. The Upload Controller uses the settings configured in this window to define when, where, and how many uploads can occur. DB Cleaner uses the settings configured in this window to define when to run DB Cleaner.

Figure 21 displays the Upload Settings window.

**Figure 21. Upload Settings window**

![Upload Settings window]

**NOTE:** Recordings for deactivated agents cannot be uploaded when an agent is deleted from the ACD. Ensure there are no recordings for that agent still on the agent PC in either the Daily or Staging folders. After Quality Management uploads all recordings for that agent, you can safely 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 32. Upload Settings fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Hours Begin</td>
<td>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.</td>
</tr>
<tr>
<td>Peak Hours End</td>
<td>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.</td>
</tr>
<tr>
<td>Max Peak Uploads</td>
<td>The maximum number of recordings that can upload simultaneously during peak hours. Must be a value from 1 to 100. This limit is set to conserve bandwidth on the network. When one upload completes, another takes its place, but there can be no more than the configured number uploading at any one time. Default = 5.</td>
</tr>
<tr>
<td>Max Off Hour Uploads</td>
<td>The maximum number of recordings that can upload simultaneously during off hours (the hours not specified as peak hours as defined by the Peak Hours Begin and Peak Hours End fields). Must be a value from 1 to 200. This limit is set to conserve bandwidth on the network. When one upload completes, another takes its place, but there can be no more than the configured number uploading at any one time. Default = 100.</td>
</tr>
<tr>
<td>Database Cleanup Time</td>
<td>The time when the DB Cleaner utility runs. This utility deletes expired recordings from the database. Must be between 00:00 and 23:59 in 1-minute increments. Choose a time when no uploads are occurring to reduce the load on the system. Default = 00:05.</td>
</tr>
<tr>
<td>Screen Server</td>
<td>(Read-only) Provides the IP address for the Screen server and the path to the screen recordings. If the AQM license is not installed, this does not appear. This section only appears after Voice and Screen services are installed on the Screen server.</td>
</tr>
<tr>
<td>Voice Server</td>
<td>(Read-only) Provides the IP address for the Voice server and the path to the audio recordings. This section only appears after Voice and Screen services are installed on the Voice server.</td>
</tr>
</tbody>
</table>
Configuration Settings Used By Services

If you change the settings on the Upload Settings window, Table 33 shows when your changes take effect.

Table 33. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload Controller service</td>
<td>The next End of Day applies the configuration settings.</td>
</tr>
<tr>
<td>DB Cleaner service</td>
<td>The next cleanup time applies the configuration settings.</td>
</tr>
<tr>
<td>FTS webapp (Jetty service)</td>
<td>Start the Jetty service.</td>
</tr>
</tbody>
</table>

Monitoring and Notification

Use the Monitoring and Notification window to enable the monitoring and notification feature, and to configure the following information.

- Method used to notify administrators/supervisors of a system problem
- Email address of the person(s) receiving notification, if you configure email as the means of notification
- Trap destinations receiving notification, if you configure SNMP as the means of notification
- If and how often a renotation of the problem should be sent out
- Types of problems that will trigger notification
Figure 22 displays the Monitoring and Notification window.

**Figure 22. Monitoring and Notification window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Monitoring/Notification Service</td>
<td>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. This check box is enabled by default.</td>
</tr>
<tr>
<td>Polling Period</td>
<td>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. <strong>NOTE:</strong> When you change the polling period, it takes one polling cycle before the new polling period goes into effect.</td>
</tr>
<tr>
<td>Use Event Viewer Notification</td>
<td>Select this check box to use the Event Viewer for displaying notification messages. This check box is enabled by default.</td>
</tr>
</tbody>
</table>
## Monitoring and Notification

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SNMP Notification</td>
<td>Select this check box to use SNMP for sending out notification messages. Note that the Windows SNMP Services must be installed to be able to use SNMP notification.</td>
</tr>
<tr>
<td>SNMP Configuration</td>
<td>Click this button to configure the SNMP connection (enabled only on the Base Services server).</td>
</tr>
<tr>
<td>Use Email Notification</td>
<td>Select this check box to use email for sending out notification messages.</td>
</tr>
<tr>
<td>SMTP Configuration</td>
<td>Click this button to configure the SMTP email connection (enabled only on the Base Services server).</td>
</tr>
<tr>
<td>Email Addresses</td>
<td>The list of email addresses to which notification is sent. Maximum = 5 email addresses.</td>
</tr>
<tr>
<td>Add</td>
<td>Click this button to add an email address.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click this button to remove an email address.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click this button to edit the selected email address.</td>
</tr>
<tr>
<td>Never</td>
<td>Choose this option if you do not want to be renotified of a problem after the initial notification.</td>
</tr>
<tr>
<td>Every N Polling Periods</td>
<td>Choose this option and enter how frequently you want renotification to occur after the initial notification. For example, if you choose to be notified every 3 polling periods, you receive the initial notification on the first polling period the problem is detected, no notification the next two polling periods, and then another notification on the next polling period. This pattern will continue as long as the problem is detected.</td>
</tr>
<tr>
<td>Every Polling Period</td>
<td>Choose this option if you want renotification to occur every polling period after the initial notification.</td>
</tr>
<tr>
<td>Available Problems</td>
<td>The list of problems that can trigger notification if enabled by using the arrow keys to move them to the Enabled Problems section. By default only one problem, QM3002, is not enabled and in this list.</td>
</tr>
<tr>
<td>Enabled Problems</td>
<td>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 the Setup button to configure the Call Detail Record (CDR) task.</td>
</tr>
</tbody>
</table>
Configuration Settings Used By Services

If you change the settings on the Monitoring and Notification window, Table 35 shows when your changes take effect.

Table 35. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mana service</td>
<td>The next polling period applies the configuration settings.</td>
</tr>
</tbody>
</table>

Configuring the SNMP Settings

Use this task to configure SNMP settings for notification.

**Task**

1. Click SNMP Configuration.

   **Step Result:** The SNMP Configuration dialog box appears (Figure 23).

   **Figure 23.** 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 IP address.
3. When you finish, click OK to save your changes.

**AFTER COMPLETING THIS TASK:**

Restart the Windows SNMP service to enable your changes.

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

**Using 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 Quality Management server.

**Figure 24. SMTP Configuration dialog box**
Table 36. SMTP Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/IP Address</td>
<td>Choose Host Name or IP Address, and then enter the host name or IP address of the SMTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used by the Mana service to communicate with the SMTP server.</td>
</tr>
<tr>
<td>Use Authentication</td>
<td>Select this check box if authentication is needed to access the SMTP server.</td>
</tr>
<tr>
<td>User</td>
<td>The user name needed to access the SMTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password needed to access the SMTP server.</td>
</tr>
<tr>
<td>From Address</td>
<td>The email address from which all notification emails will come.</td>
</tr>
<tr>
<td>Emergency Address</td>
<td>The email address to which notification is sent if the Quality Management database is down when the Mana service attempts to get its initial configuration. The notification email addresses configured in the Monitoring and Notification window are stored in the Quality Management database, and thus will not be functional in the event that the Quality Management database is unavailable when the Mana service first starts. If the Mana service has already obtained a valid configuration from the Quality Management database, and then the Quality Management database goes down while the Mana service is running, the Mana service will use the valid configuration it already has. As a result, the notification that the Quality Management database is down will go to the configured email address, not to the emergency address.</td>
</tr>
</tbody>
</table>

**Configuring the SMTP Settings for Email**

Use this task to configure SMTP settings for email.

**TASK**

1. On the Base Services server, start Site Configuration Setup (PostInstall.exe).

2. Navigate to the Monitoring and Notification window.

3. Click SMTP Configuration.
STEP RESULT: The SMTP Configuration dialog box appears (Figure 25).

Figure 25. SMTP Configuration dialog box

4. Complete the fields, and then click OK.

Adding a Notification Email Address

Use this task to add a notification email address.

TASK

1. In the Monitoring and Notification window’s Notification section, click Add.

STEP RESULT: The Add Email Address dialog box appears (Figure 26).

Figure 26. 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.
Using Notification Triggers

Currently, only one notification trigger requires configuration: Problem ID QM3002. This trigger compares data in the Unified CM’s Call Detail Record database (for Unified CM version 4.0) or CAR Report (for Unified CM versions 5.0 and 6.0) with the Quality Management database. Specifically, it compares the call records in the Unified CM with the call records in Quality Management. If there is a discrepancy, notification is sent.

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.

Table 37. Configuration dialog box fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster &lt;number&gt; &lt;IP address&gt;</td>
<td>Displays the CDR connection information and ignored extensions associated with the cluster. The number of cluster tabs that appear depend on the number of clusters configured for this system. The fields listed under the Cluster tab applies only to that cluster.</td>
</tr>
<tr>
<td>Unified CM Version</td>
<td>Select the version of the Cisco Unified CM you are using.</td>
</tr>
<tr>
<td>Host Name/IP Address</td>
<td>Choose host name or IP address, and then enter the information for the Unified CM.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>Enabled only if using Unified CM 4.x. The instance name of the Unified CM database. Usually the default instance of the CDR database is used, so this field can be blank.</td>
</tr>
<tr>
<td>Username</td>
<td><em>(Unified CM 6.x, 7.x, 8.x)</em> The name of the user with rights to access the CAR reports.</td>
</tr>
<tr>
<td>Password</td>
<td><em>(Unified CM 6.x, 7.x, 8.x)</em> The password of the user with rights to access the CAR reports.</td>
</tr>
<tr>
<td>Ignored Extensions</td>
<td>Displays the list of ignored extensions. Quality Management does not send notifications about extensions that appear in this list. Select one of the following options to modify the extensions that appear in this list.</td>
</tr>
<tr>
<td></td>
<td>• Add—Add a new extension to the list.</td>
</tr>
<tr>
<td></td>
<td>• Remove—Delete an extension from the list.</td>
</tr>
<tr>
<td></td>
<td>• Edit—Modify a selected extension in the list.</td>
</tr>
<tr>
<td>Properties</td>
<td>The fields listed in the Properties section apply to all clusters.</td>
</tr>
<tr>
<td>Minimum Misses</td>
<td>Lowest number of missed CDRs required to trigger notification.</td>
</tr>
</tbody>
</table>
CDR Information Formats for the QM3002 Notification Trigger

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify on users that are logged in</td>
<td>When you select this option, Quality Management only generates notifications about users who are currently logged in to Cisco Unified Workforce Optimization. This only applies to the Desktop Recording (Endpoint) service.</td>
</tr>
<tr>
<td>Display Type</td>
<td>Choose one of the following options.</td>
</tr>
<tr>
<td></td>
<td>• Summary Only—displays 1 row per agent with misses that meet the above criteria.</td>
</tr>
<tr>
<td></td>
<td>• Details (Tab Delimited)—displays each missed CDR in tab delimited format.</td>
</tr>
<tr>
<td></td>
<td>• Details (Plain Text)—displays each missed CDR in text format.</td>
</tr>
</tbody>
</table>

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

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

**Summary Only**

<table>
<thead>
<tr>
<th>Status Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time: 01/11/2008 15:25:53</td>
</tr>
<tr>
<td>End Time: 01/11/2008 16:25:53</td>
</tr>
<tr>
<td>Extensions with Missed Calls:</td>
</tr>
<tr>
<td>Ext</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1545</td>
</tr>
<tr>
<td>2201</td>
</tr>
</tbody>
</table>
Detail (Tab Delimited)

Status Report
Start Time: 01/11/2008 15:23:41
End Time: 01/11/2008 16:23:41
Extensions with Missed Calls:
  Ext  Agent  Found   Missed   % Missed
  1545  JonesM  0       8        100%
  2201  SmithB  0       16        100%
Missed Calls (all times in GMT):
  CallID  Agent  Ext  ANI  DNIS  StartTime  Duration
  16778554 JonesM  1545  2671  1545  01/11/2008  03:29:36  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
Enabling or Disabling a Notification Trigger

**PREREQUISITE**

When enabling the QM3002 notification trigger:

- CDR must be correctly configured in the Unified CM Administration web application.
  - Unified CM 6.x, 7.x, and 8.x: See Serviceability > Tools. In these versions, there is no CDR database. Instead, the CAR reports (CDR export) are used. Set up CAR so that it updates its information as frequently as possible, at a minimum, at less than 30-minute intervals. Create a CAR user and enter that user in the Recording CDR Configuration dialog.
- Archiving must be enabled in Quality Management.

This task describes how to enable and disable a notification trigger.

**TASK**

- To enable a task notification trigger, choose a trigger from the Available Problems section and click >. The trigger moves to the Enabled Problems section.
- To enable all task notification triggers, click >>. All triggers move to the Enabled Problems section.
- To disable a task notification trigger, choose a trigger from the Enabled Problems section and click <. The trigger moves to the Available problems section.
- To disable all task notification triggers, click <<. All triggers move to the Available problems section.
Configuring the QM3002 Notification Trigger

This task describes how to configure the QM3002 notification trigger.

**TASK**

1. Click Setup next to the QM3002 notification trigger in the Enabled Problems section.

   **STEP RESULT:** The Configuration dialog box appears (Figure 27).

**Figure 27. Configuration dialog box**

2. Select the version of the Cisco Unified CM you are using from the drop-down list.

3. Choose Host Name or IP Address, and then enter the information for the Unified CM.

4. If the Instance Name field is enabled, enter the instance name of the Unified CM database.

   **ADDITIONAL INFORMATION:** The Instance Name field is only enabled if you are using Unified CM 4.x. Usually the default instance of the CDR database is used, so this field can be blank.

5. Enter the username and password.
ADDITIONAL INFORMATION: For Unified CM 6.x, 7.x, or 8.x, enter the name and password of the user with rights to access the CAR reports.

6. Add the extensions that you do not want to receive notifications.

7. Configure the properties for the notification.

8. Click OK.

Adding an Ignored Extension

This task describes how to add an extension to the Ignored Extension list.

TASK

1. In the Ignored Extensions section, click Add.

STEP RESULT: The Add Extension dialog box appears (Figure 28).

Figure 28. Add Extension dialog box

2. Enter the extension in the field, and then click OK.

Modifying an Ignored Extension

This task describes how to modify an extension in the Ignored Extension list.

TASK

1. In the list of CDR connections, select the connection you want to edit.

2. Click Edit.
**STEP RESULT:** The Edit Extension dialog box appears (Figure 29).

![Edit Extension dialog box](image)

3. Make the necessary changes in the Edit Extension dialog box, and then click OK.

**Removing an Ignored Extension**

Use this task to remove an extension from the Ignored Extension list.

**TASK**

- Select an extension from the Ignored Extensions list and click Delete.

**Examples of Notification Configuration Problems**

The following setup examples illustrate what happens when you configure the Notification Trigger Configuration as described.

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

Agent  
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 $\frac{2}{8 + 2} = 20\%$. No notification would be made because neither the Miss Threshold or the Minimum Misses criteria were met.  
Agent B: No notification would be made because the Minimum Misses criterion (5) was not met.  
Agent C: The missed percentage is $\frac{8}{2 + 8} = 80\%$. Notification is made because the Miss Threshold and the Minimum Misses criteria 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 Quality Management but does not have the Desktop Recording service installed, or the phone is not daisy-chained properly.  
Effect | Notification will be made on Agent A's extension, with the agent listed as "Unknown" because there is no cross-reference between the agent and extension until the Desktop Recording service is configured. |

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

**NOTE:** Agent team association and whether a team is configured for archiving are determined from the time the CDR task is run, not from the time of the call in question. This could result in either false positives or false negatives if a team's archiving status changes, or if an agent's team membership changes during the period the CDR task is examining.
When a notification is received, look at the DNs/Agents that show missed calls. A large number of agents with missed calls might indicate a Quality Management service failure. The possible services with issues are:

- CTI service
- Upload Controller
- DB Proxy service (on the Database server)

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

**RTP Filters**

Use the Real-time Transport Protocol (RTP) Filters window to filter voice packets. For example, use RTP filters when Quality Management is installed in an environment where Cisco Agent Desktop is present and you want to avoid getting duplicate RTP packets when a Cisco Desktop Supervisor is monitoring or recording calls.

*Figure 30* displays the RTP Filters window.
Table 38. RTP Filters fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Filter Type</td>
<td>The type of RTP filter in use. The following options are available.</td>
</tr>
<tr>
<td></td>
<td>• IP Port—If selected, the RTP Filter IP/Port field is limited to valid IP</td>
</tr>
<tr>
<td></td>
<td>port ranges (1-65535).</td>
</tr>
<tr>
<td></td>
<td>• IP Address—If selected, the RTP Filter IP/Port field is limited to valid</td>
</tr>
<tr>
<td></td>
<td>IP addresses (IPv4).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Wildcards and ranges are not allowed in this field.</td>
</tr>
<tr>
<td>RTP Filter IP/Port</td>
<td>The value for the RTP filter. If the RTP Filter Type is IP Port, a port</td>
</tr>
<tr>
<td></td>
<td>number appears in this field. If the RTP Filter Type is IP Address, an</td>
</tr>
<tr>
<td></td>
<td>IP address appears in this field.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Hostnames, wildcards, and ranges are not allowed in this field.</td>
</tr>
</tbody>
</table>

Configuration Settings Used By Services

If you change the settings on the RTP Filters window, Table 39 shows when your changes take effect.

Table 39. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Recording Service</td>
<td>Restart the client application.</td>
</tr>
</tbody>
</table>

RTP Filter Guidelines

Use the following guidelines when adding or editing RTP filters.

- CAD ports appear in the list of RTP filters by default. If you are using CAD, you must also enter the IP address of the CAD Recording server.
- The number of rows that can appear in the list of RTP filters is limited to 1000.
- Do not enter the same filter twice. An error appears if you enter the same filter twice.
Adding an RTP Filter

Use this task to add an RTP filter to the list of RTP filters.

**TASK**
1. From the RTP Filters window, click Add.

**STEP RESULT:** The RTP Filter dialog box appears ([Figure 31](#)).

![RTP Filter dialog box](image)

2. Choose one of the following options from the RTP Filter Type drop-down list.
   - IP Port
   - IP Address
3. Enter the port number or IP address for the RTP Filter Type in the RTP Filter IP/Port field.
4. Click OK to save your changes and dismiss the dialog box.

**STEP RESULT:** The new RTP filter appears in the list of RTP filters.

Editing an RTP Filter

Use this task to edit an existing RTP filter.

**TASK**
1. Select an RTP filter from the list.

**STEP RESULT:** The selected filter is highlighted in blue and the Edit button is enabled.
2. Click the Edit button.
STEP RESULT: The RTP Filter dialog box appears (Figure 32).

Figure 32. RTP Filter dialog box

3. Choose one of the following options from the RTP Filter Type drop-down list.
   - IP Port
   - IP Address

4. Enter the port number or IP address for the RTP Filter Type in the RTP Filter IP/Port field.

5. Click OK to save your changes and dismiss the dialog box.

STEP RESULT: The modified RTP filter appears in the list of RTP filters.

Deleting an RTP Filter

Use this task to delete an RTP filter from the list of RTP filters.

TASK
1. Select an RTP filter from the list.

   STEP RESULT: The selected filter is highlighted in blue and the Delete button is enabled.

2. Click the Delete button.

   STEP RESULT: The RTP filter is removed from the list of RTP filters.
Status

The Status window reports the version of the installed Quality Management components.

Configuration Settings Used By Services

If you change the product version, Table 40 shows when your changes take effect.

Table 40. When services start using the changed configuration settings

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration Settings Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload Controller</td>
<td>Periodically check for a version mismatch.</td>
</tr>
<tr>
<td>service</td>
<td></td>
</tr>
</tbody>
</table>

Entering Configuration Data in Update Mode

There are two ways to change Configuration Setup data after it is initially entered.

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

When Configuration Setup starts, it runs in Update Mode.

Rules for Upgrading or Modifying the Unified CC Database in Update Mode

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

- Do not change the location of the Unified CCX database after initial setup. If you do, you might be unable to access Quality Management historical data if the structure and contents of the new database is not the same as that of the old database.
- Stop the Sync Service and disable this service on startup to protect the Quality Management database before you upgrade or rebuild the Unified CCX database.
Stopping the Sync Service Before Upgrading the Unified CCX Database

Use this task to stop the Sync Service, before you upgrade the Unified CCX database.

**TASK**


**STEP RESULT:** The Services window appears.

2. Right-click Quality Management Sync Service and choose Stop.


4. Choose Disabled from the Startup Type drop-down list, and click OK to save your changes.

5. Upgrade or rebuild the Unified CCX database.

6. Return to the Services window, right-click Quality Management Sync Service and choose Start.

7. Right-click Quality Management Sync Service again, choose Automatic from the Startup Type drop-down list, and then click OK to save your changes.

**STEP RESULT:** This action enables the Sync Service on startup.

**NOTE:** Do not start Sync Service and enable the Sync Service for the hardware profile until both Unified CCX Administration databases (if using High Availability) Recording are running and synchronized because the Sync Service reads data from the Unified CCX database. Failing to do so could potentially deactivate users if there is a problem with the Unified CCX upgrade or rebuild.

8. Verify the teams and agents in the upgraded Unified CCX appear correctly.

Changing the Base Server

**TASK**

1. From the Site Configuration Setup tool, choose File > Choose Base Server.

**STEP RESULT:** The Quality Management Configuration Setup dialog box appears.

2. Enter the IP address of Quality Management Base server.
3. Enter the IP address of the Cisco Unified Workforce Optimization Container.

**ADDITIONAL INFORMATION:** The Cisco Unified Workforce Optimization Container is located on the Base server. Enter the IP address of Quality Management Base server.

4. Choose one of the following options:

   - If you are running Site Configuration Setup on the Quality Management Base Services server, choose the IP address of the Quality Management Base Services server from the IP Address for local Services drop-down list, and then click OK.

   - If you are running Site Configuration Setup on a different server, choose the IP address for the server from the IP Address for local Services drop-down list, and then click OK.

**ADDITIONAL INFORMATION:** For example, if you want to run Network Recording on a different server and installed the Network Recording service and Monitor service on the server, choose the IP address for the Network Recording server from the IP Address for local Services drop-down list. If the computer has multiple NICs, multiple addresses appear in the IP Address for local Services drop-down list. Choose the IP address used for network traffic.

### Changing Quality Management Configuration Data in Update Mode

**Use this task to change the configuration data in update mode.**

**TASK**

1. Start Quality Management Setup by running the PostInstall.exe.

   **ADDITIONAL INFORMATION:** This executable is located in the C:\Program Files\Cisco\WFO_QM\bin folder.

2. Select the window you want to modify from the left pane, enter the new data in the right pane, and then click Save on the toolbar or File > Save from the menu bar.

   - You can display the windows in any order you wish.

   - If you modify something in a window, you must click Save to save your changes before you move on to another window.

   - If you make a change to a window but need to change back to the original setting, click the Revert to Saved button on the toolbar. This discards any
changes you made but have not saved yet, and reverts the window back to the last saved version.

3. When you finish, choose File > Exit or click Close.

**STEP RESULT:** Configuration Setup closes.

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

### Site Configuration Setup Tools

Site Configuration Setup provides a number of tools you can use to update your site information. These tools are available through the Tools menu. These tools normally run during the initial installation of Quality Management.

The Tools menu, in Site Configuration Setup, only enables tools when the tools are available on there server where you are running the Site Configuration Setup tool (Figure 33).

**Figure 33.** Site Configuration Setup tools
The following table displays the available tools and the servers on which they are located.

**Table 41.** Tool availability in the Site Configuration Setup tool

<table>
<thead>
<tr>
<th>Tool</th>
<th>Base Server</th>
<th>Database Server</th>
<th>Voice and Screen Server</th>
<th>CTI Server</th>
<th>Rec &amp; Mon Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Local Services</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Create Database Catalogs</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generate Info for MSI Clients</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download/Install JTAPI</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Encrypt Audio Files</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Set Recording Home Directory</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Generate SSL Certificates</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Test CTI Service(s)</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Display Metadata Encryption Key</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Choose Monitor Adaptor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Remove Recording Services</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Configure Local Servers</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Start Local Services**

This tool offers a convenient way to start all the Quality Management that are on the local computer. You can run this tool any time. However, you should notify users because restarting services might cause outages.
Create Database Catalogs

This tool creates a new Quality Management database if one does not exist or updates an existing database to the latest schema version without overwriting any existing data. You can use this tool to recreate your Quality Management database if you have no backup database and your database was corrupt and you deleted it. This tool populates a fresh database when the Unified CCX and Data API sync with it.

Generate Info for MSI Clients

This tool updates the information required by the MSI client installation programs to successfully install Calabrio Screen Player Plug-in, the Desktop Recording service, and Quality Management Administrator.

Download/Install JTAPI

Use this tool when you upgrade Unified CM. This tool downloads and installs JTAPI.

Encrypt Audio Files

Cisco QM 2.1 did not encrypt audio files. Encrypted files appear in Cisco QM 2.7(2) or later. When upgrading from version 2.1 to 8.5, some audio files might remain in the staging folders on the client machines during the upgrade process and upload after the upgrade without encryption.

This tool enables you to encrypt any unencrypted audio files. Run this tool only after you upgrade all client desktops to Quality Management 8.5. All audio files are encrypted after you run this tool.

Set Recording Home Directory

This tool displays the Recording Location window. Use this window to change the recording storage location. Run this step when upgrading from the Basic license to the Advanced license.

**NOTE:** If you change the storage location from local to external storage, you must first uninstall Screen Recording Gateway on the server that hosts the Voice and Screen services (from the Control Panel’s Add or Remove Programs, remove PROXY Pro Gateway). When you run the Set Recording Home Directory tool, Quality Management automatically reinstall the DB Proxy service.
Changing the Recording Location in Update Mode

Use this task to change the location of the contact recordings.

PREREQUISITE

- If you change the storage location from local to external storage, you must first uninstall the DB Proxy service on the server that hosts the Recording Voice and Screen services (in Control Panel’s Add or Remove Programs, remove PROXY Pro Gateway). When you run the Set Recording Home Directory tool, the DB Proxy service reinstall automatically.
- If you select an external storage location, you must provide a username and password to access the external storage location. The user must meet these requirements:
  - The local server knows the user. If you are using domains, the user must be a trusted domain user.
  - A domain user must belong to a domain that is trusted by the local server. This means the Recording Server must belong to the same domain as the user or a domain that is trusted by the user’s domain.
  - The user must be able to log on as a service.
  - For external screen storage and external screen playback to work, you must provide a domain user that has read/write access to the local Quality Management server and the external storage system.

TASK

1. From the Configuration Setup tool, choose Tools > Set Recording Home Directory.

   STEP RESULT: The Recording File Storage Location window appears.

2. Select if you want to store recordings in a local or external storage location, and then enter the desired location in the IP Address and Storage Location fields.

3. If you selected an external location, enter the username and password. If the user is a domain user, enter the name with the format <domain>\<username>.

4. Click OK.

Generate SSL Certificate

This tool generates a security certificate for the File Transfer Servlet (FTS) and Cisco Unified Workforce Optimization-generated reports. Use this tool if your certificate is corrupt or if the IP address of the server changes (the user sees a Security Alert dialog box whenever the FTS or Reports runs). This tool is available only when you run Site
Configuration Setup on the Quality Management server (for reporting) and the Voice and Screen Services server (for FTS).

When you run the tool, you see a Security Alert dialog box. Click View Certificate to display the Certificate dialog box, and then Install Certificate to install a new certificate.

Test CTI Service(s)

This tool verifies that the local CTI Service has the correct JTAPI and accepts connections. The tool makes a request to each CTI Service and, if all succeed, returns a success message. If any requests fail, Quality Management reports the failure and lists which succeed. The reports are available from Cisco Unified Workforce Optimization.

Display Metadata Encryption Key

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

Choose Monitor Adaptor

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

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

Remove Recording Services

Use this tool to finalize the removal of Network Recording service and Monitor service servers by removing them from database. Do this after you uninstall the services from the server.

Configure Local Servers

Use this tool to update server profiles for all local services with the latest properties.

**NOTE:** If you changed the IP address for the Network Recording service or the Monitor service, you need to run Remove Recording Services to remove the old IP addresses.
Setting Up NT Authentication for the Cisco Unified CC Database

If you select NT Authentication on the Unified CC Database window in Site Configuration Setup, you must perform the following procedure to support NT authentication for the Unified CC database.

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

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

1. Set up NT users who will be used to connect to the database.
2. Allow the user access to the Unified CC database.
3. Verify the connection.

Setting Up NT Users

Follow these steps to set up the NT users who can connect to the database. The server and the server must know the user, and the server cannot be on a domain.

On the server:

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

Adding an NT User

Use this task to add an NT user.

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

STEP RESULT: The user appears in the list of users.
Adding an NT User to a Group

Use this task to add an NT user to a group.

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

Verifying the Connection

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

**TASK**
1. Start Quality Management Administrator.
2. Click Personnel > User Administration, and select the Unlinked Users tab (for systems that use Active Directory) or the Unconfigured Users tab (for systems that do not use Active Directory).

**STEP RESULT:** If there are users listed there, the synchronization worked.

Allowing the User Access to the Cisco Unified CC Database

Follow these steps to allow the user to access the database.

**TASK**
1. On the computer that hosts the database, open the SQL Server Enterprise Manager and navigate to the Security node under the Unified CC database instance (which might be the default instance).

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

2. To create a new login:
   a. Right-click Logins and choose New Login from the popup menu.
   b. On the General tab, enter the user name in the Name field. In the Authentication section, select Windows Authentication, select or enter the user’s Windows domain in the Domain field, and select Grant access.
   c. Click OK to add the new login to the list.

3. Right-click the login and choose Properties from the popup menu.

4. On the Database Access tab, select <dbname>_sideA in the list of databases. In the Database Roles pane, select db_datareader.

5. Repeat step 4 for <dbname>_sideB.

6. Click OK.
Supporting Asian Languages

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

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

Installing Supplemental Language Support

**TASK**
1. From the Quality Management Base Services server, choose Start > Settings > Control Panel.

   **STEP RESULT:** The Control Panel window appears.

2. Double-click Regional and Language Options.

   **STEP RESULT:** The Regional and Languages Options window appears.

3. Click the Languages tab.

4. Select the Install files for East Asian languages check box.

   **STEP RESULT:** The Install Supplemental Language Support dialog box appears.

5. Click OK to dismiss the dialog box, and then click Apply.

6. Follow the prompts to install the fonts.

7. Restart the Quality Management Base Services server.

   **ADDITIONAL INFORMATION:** The server might automatically restart after installing the fonts.
8. From Control Panel, double-click Fonts.

**STEP RESULT:** The Fonts window appears.

9. Select and copy the font you just added.
   
   - batang.tcc (Russian and Korean)
   - mingliou.tcc (Chinese and Japanese)

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

11. Restart the Quality Management Jetty service.
Upgrading from Previous Versions

To upgrade from a previous version, choose one of the following options.

<table>
<thead>
<tr>
<th>Previous Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Management 8.0(2)</td>
<td>Uninstall Quality Management 8.5, then install Quality Management 8.0(2)</td>
</tr>
<tr>
<td>Quality Management 2.7</td>
<td>Uninstall Quality Management 2.7, then install Quality Management 8.5</td>
</tr>
<tr>
<td>Quality Management 2.6</td>
<td>Uninstall Quality Management 2.6, then install Quality Management 8.5</td>
</tr>
<tr>
<td>Quality Management 2.5</td>
<td>Upgrade to Quality Management 2.7, then uninstall Quality Management 2.7, and then install Quality Management 8.5</td>
</tr>
<tr>
<td>Quality Management 2.4</td>
<td>Upgrade to Quality Management 2.6, then uninstall Quality Management 2.6, and then install Quality Management 8.5</td>
</tr>
<tr>
<td>Quality Management 2.3</td>
<td>Upgrade to Quality Management 2.6, and then uninstall 2.6, and then install Quality Management 8.5</td>
</tr>
</tbody>
</table>

**NOTE:** When upgrading to Quality Management 2.6 or Quality Management 2.7, consult the appropriate *Installation Guide* for installation instructions.

See “Upgrading Quality Management 2.6 or 2.7 to Quality Management 8.5” on page 144 for upgrade instructions.

Consult the *Services Release Notes for Cisco Unified Workforce Optimization Quality Management* for any last minute changes to the upgrade procedure.

Workflows and Retention Periods

In all releases prior to 2.7(2), retention periods were global for all contacts. Quality calls had Scored, Unscored, HR, Training, and Tagged retention periods. Archive calls had a single Archive retention period. Tagged retention periods, configured under the Quality Management node, applied to tagged quality management calls and tagged archive-only calls. In this release, you can configure retention periods per workflow. Also, you can configure Tagged retention periods separately for quality workflows and archive workflows.
When upgrading to Quality Management 8.5 from 2.6, Quality Management assigns the retention periods configured before the upgrade to all existing workflows. After upgrading to Quality Management 8.5, you can change these retention periods per workflow. You can modify the retention periods under the Quality Management > Workflows and Archive > Workflows nodes in Quality Management Administrator after the upgrade is complete. Quality Management assigns retention periods configured before the upgrade to calls recorded before the upgrade. However, you cannot change the retention periods for these calls.

These changes occur after you configure the Quality Management Database step in the Site Configuration Setup tool. A progress bar (Figure 34) appears when Quality Management implements these changes.

Figure 34. Assigning Workflow Retention progress bar

Upgrade Guidelines

When you upgrade from Cisco Quality Management to Quality Management follow these guidelines.

NT Authentication

If you upgrade from Quality Management 2.7(3) and you are using NT authentication, you must select the NT option in the Cisco Unified CC Database window, and enter a login ID and password.

PrxgpxNT.dll Failed to Register

If you see a dialog box containing the following message when performing an over-the-top upgrade on a machine running both Quality Management Desktop and Desktop Recording service for 2.6, dismiss the dialog to successfully complete the installation.

PrxgpxNT.dll failed to unregister

There are no known side effects associated with this error message.
Upgrading Quality Management 8.0(2) to Quality Management 8.5

Use the following task to upgrade from Quality Management 8.0(2) to Quality Management 8.5.

**TASK**

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

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

   See “Backing Up the Quality Management Databases” on page 185 for instructions.

2. Remove Quality Management 8.0(x) or 8.5(x).

   **ADDITIONAL INFORMATION:** See “Removing Quality Management 8.5” on page 155 for instructions.

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

3. Manually reboot the server.

4. Install Quality Management 8.5 (x+) on the Base Services server and select the Enable automatic updates for all clients check box on the Enterprise Settings window in the Configuration Setup utility.

   **ADDITIONAL INFORMATION:** Selecting the Enable automatic updates for all clients check box ensures that Quality Management automatically updates the client desktops after you install Quality Management 8.5(x+).

   See “Installing Quality Management” on page 63 for instructions.

5. Restore the Quality Management database.

   **ADDITIONAL INFORMATION:** See “Restoring the Quality Management Database” on page 186 for instructions.
Upgrading Quality Management 2.6 or 2.7 to Quality Management 8.5

Use the following task to upgrade from Quality Management 2.6 or 2.7 to Quality Management 8.5.

**TASK**


   **ADDITIONAL INFORMATION:** Quality Management 8.5 no longer requires the LDAP database. You need a clean copy of the LDAP database if you intend to downgrade from Quality Management 8.5.

   See “Backing Up the Quality Management Databases” on page 185 for instructions.

2. Remove Quality Management 2.6 or 2.7.

   **ADDITIONAL INFORMATION:** See “Removing Quality Management 2.6 or 2.7” on page 151 for instructions.

3. Manually reboot the server.

4. Install Quality Management 8.5 on the Base Services server and select the Enable automatic updates for all clients check box on the Enterprise Settings window in the Site Configuration Setup utility.

   **ADDITIONAL INFORMATION:** Selecting the Enable automatic updates for all clients check box ensures that Quality Management automatically updates the client machines after you install Quality Management 8.5.

   See “Installing Quality Management” on page 63 for instructions.

5. Restore the Quality Management database.

   **ADDITIONAL INFORMATION:** See “Restoring the Quality Management Database” on page 186 for instructions.
Upgrading the Client Applications

**PREREQUISITE**

Verify Java JRE version 1.6.0_13 or greater is installed on the client machines.

When you upgrade from Quality Management 2.6 or 2.7 to Quality Management 8.5, you must remove the existing Quality Management Desktop Recording from each client machine and replace them with the Calabrio Screen Player Plug-in and Desktop Recording service. Quality Management 8.x replaced the Quality Management Desktop with the Cisco Unified Workforce Optimization.

**TASK**

1. Uninstall the following applications from each client machine.
   - Quality Management Desktop
   - Quality Management Desktop Recording
   - Quality Management Administrator—from the administrator’s machine only

   **ADDITIONAL INFORMATION:** See “Removing a Quality Management Application” on page 152 for more instructions.

2. Install the following applications from each client machine.
   - Calabrio Screen Player Plug-in
   - Desktop Recording service
   - Quality Management Administrator—on the administrator’s machine only

   **ADDITIONAL INFORMATION:** See “Installing Client Applications for Quality Management” on page 66 for more instructions.

Testing the Upgrade on Client Machines

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

**PREREQUISITE**

If you configured your site for Desktop Recording (Endpoint), you must install the Desktop Recording service on the client machines you are testing.
Upgrading from Previous Versions

Verifying the Upgrade is Installed Correctly on the Quality Management Server

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

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

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

Verifying the Upgrade is Installed Correctly on the Quality Management Server

Verify Quality Management 8.5 appears in the list of Add or Remove Programs.

TASK
1. Select Start > Add or Remove Programs.

   **STEP RESULT:** Quality Management should appear in the list.

2. Verify the version is correct by clicking Click Here for Support Information.

   **STEP RESULT:** The version appears in the Support Info dialog box.
Installing a Service Release or Patch

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

**engineering-test (ET)**
An installable component that contains the files needed to assist developers when diagnosing a problem. An ET can contain server and/or client files. Always install an ET on the Quality Management Base Services server. If the ET also contains client files, install the ET directly on the client machine.

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

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

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

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

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

**maintenance release (MR)**
Contains the base release of the product. Always install the MR on the Quality Management server. The Quality Management server uses the automated update feature, when you enable this feature, to update the clients when you install an MR on the Quality Management server. If the MR contains no fixes for the client side, the automated update feature does not update the clients.
You install each MR separately and each MR appears in the Add/Remove Programs window. Separate installation of MRs allows rollback to a previous state. If an MR is server side only, the Add/Remove Program title includes “(Server only).”

Guidelines for Installing a Patch (SR or ES)

Use the following guidelines when installing and ES or SR.

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

Installing an Patch (ES or SR)

Use this task to install an ES or SR on the Quality Management server. If the ES or SR includes client-side fixes, and the automatic update feature is available, then the automatic update feature will update the clients.

**PREREQUISITE**

Remove any engineering tests (ETs) installed on the Quality Management server. See “Rolling Back to a Previous State” on page 149 for instructions.

**TASK**

1. Download the executable to the Quality Management Server.

**ADDITIONAL INFORMATION:** Before installing the SR, the SR install checks for any unknown ESes on the Quality Management server. If the SR install finds an unknown ES, the SR install displays a message and stops the installation process. Uninstall the unknown ES on the Quality Management server and try again.

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

*STEP RESULT:* The executable installs the files for the ES or SR.

**Rolling Back to a Previous State**

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

**PREREQUISITE**

Cisco builds each SR, and ES sequentially. When you roll back to a previous state, you must remove the SR, or ES in the order you installed them.

**TASK**

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

*STEP RESULT:* The Control Panel window appears.

2. Double-click Add or Remove Programs.

*STEP RESULT:* The Add or Remove Programs window appears.

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

*ADDITIONAL INFORMATION:* If there are multiple patches applied, you must remove the patches in the reverse order they were installed. Always remove the patch that displays a “Remove me first” message first. When your remove the first patch that displayed this message, the next patch you can remove will now display the “Remove me first” message, and so on. Continue removing patches until you reach the desired state.

*STEP RESULT:* The SR, ES, or ET is removed from the Quality Management Base Services server.
Removing Quality Management 2.6 or 2.7

If you are upgrading from Quality Management 2.6 or 2.7 to Quality Management 8.5, you must uninstall Quality Management before you install Quality Management.

Uninstall Quality Management in the following order:

1. Clear the Enable automatic updates for all Quality Management clients check box on the Enterprise Settings window in Quality Management Administrator
2. Quality Management service release, if any
3. Quality Management client applications (Quality Management Administrator and Quality Management Desktop)
4. Quality Management Desktop Recording service
5. Quality Management from the Quality Management server. This includes the following services:
   • Quality Management CTI service
   • Quality Management DB Cleaner service
   • Quality Management DB Proxy service
   • Quality Management LDAP Monitor service
   • Quality Management Monitoring and Notification (Mana) service
   • Quality Management Monitor service
   • Quality Management Network Recording service
   • Quality Management Sync service
   • Quality Management Tomcat service
   • Quality Management Upload Controller
6. Cisco Unified Communications Manager JTAPI client
7. Proxy PRO Gateway service

A user must log in as an administrator in order to remove any Quality Management applications.

Recordings are not uploaded from client or server computers when you remove Cisco Quality Management. They are maintained in the folder located at:

C:\Program Files\Common Files\SQM\Recordings
The default location on the storage server for uploaded recordings is:

C:\Program Files\Common Files\QM\Recordings

Note that these are the default locations and that your recordings might be stored in custom location.

**NOTE:** A user must log in as an administrator in order to remove any Quality Management applications.

### Removing a Quality Management Application

Use this procedure to uninstall the components identified in “Removing Quality Management 2.6 or 2.7” on page 1.

**TASK**

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

**STEP RESULT:** Windows removes the application.

**NOTE:** If you have multiple client applications for Quality Management installed on one computer, and wish to uninstall one application and leave the rest, you must uninstall all of the applications, reboot your computer, and then reinstall the desired set of applications. The applications share certain third party files, and uninstalling one application may remove files needed by the remaining applications.

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

### Removing the Quality Management Databases

Using the Windows Control Panel to remove services does not remove the Quality Management database (SQMDB). If you intend to reinstall or upgrade Quality Management, and you want to retain historical data, you must not remove the Quality
Management database. However, if you want to remove Quality Management completely, follow this procedure to remove the database.

**TASK**

1. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.

2. In the left navigation pane, expand the Databases node and right-click SQMDB.

3. From the popup menu, choose Delete.

**STEP RESULT:** the Delete Object window appears (Figure 35).

**Figure 35.** Delete Object window

4. Select the Close existing connections check box and then click OK.
Verifying Quality Management was Removed Correctly

Use the following task to verify you successfully removed Quality Management 2.6 or 2.7.

**TASK**

1. From the server, choose Start > Run.
   
   **STEP RESULT:** The Run dialog box appears.

2. Type `regedit` in the Open field and click OK.
   
   **STEP RESULT:** The Registry Editor window appears.

3. Verify the SQM folder does not appear under `HKEY_LOCAL_MACHINE/SOFTWARE/Spanlink`.
   
   - If the SQM folder exists, delete the folder.
   - If the SQM folder does not exist, you successfully removed Quality Management.
Removing Quality Management 8.5

Uninstall Quality Management in the following order:

1. Clear the Enable automatic updates for all Quality Management clients check box on the Enterprise Settings window in Quality Management Administrator
2. Quality Management ETs, if any
3. Quality Management ESes, if any
4. Quality Management SRs, if any
5. Quality Management client applications
6. Quality Management Desktop Recording service
7. Quality Management from the Quality Management server. This includes the following services:
   • Quality Management CTI service
   • Quality Management Data API service
   • Quality Management DB Proxy service
   • Quality Management Jetty service
   • Quality Management Mana service
   • Quality Management Monitor service
   • Quality Management Network Recording service
   • Quality Management Sync service
   • Quality Management Upload Controller
8. Cisco Unified Communications Manager JTAPI client
9. PROXY Pro Gateway service

Recordings are not uploaded from client or server computers when you remove Quality Management. They are maintained in the folder located at:

C:\Program Files\Common Files\SQM\Recordings

The default location on the storage server for uploaded recordings is:

C:\Program Files\Common Files\QM\Recordings

Note that these are the default locations and that your recordings might be stored in custom location.
NOTE: A user must log in as an administrator in order to remove any Quality Management applications.

Removing a Quality Management Application

Use this procedure to uninstall the components identified in “Removing Quality Management Monitoring and Recording Services 8.5 8.6” on page 1.

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

STEP RESULT: Windows removes the application.

NOTE: If you have multiple client applications for Quality Management installed on one computer, and wish to uninstall one application and leave the rest, you must uninstall all of the applications, reboot your computer, and then reinstall the desired set of applications. The applications share certain third party files, and uninstalling one application may remove files needed by the remaining applications.

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

Removing the Quality Management Databases

Using the Windows Control Panel to remove services does not remove the Quality Management database (SQMDB). If you intend to reinstall or upgrade Quality Management, and you want to retain historical data, you must not remove the Quality Management database. However, if you want to remove Quality Management completely, follow this procedure to remove the database.

TASK
1. On the server that hosts the Quality Management database, launch and log in to Microsoft SQL Server Management Studio.
2. In the left navigation pane, expand the Databases node and right-click SQMDB.

3. From the popup menu, choose Delete.

**STEP RESULT:** The Delete Object window appears (Figure 36).

**Figure 36. Delete Object window**

4. Select the Close existing connections check box and then click OK.
Removing Quality Management 8.5
Removing the Quality Management Databases
Checklists and Activities

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

Pre-Installation Checklists

Use the pre-installation checklists to prepare for a Quality Management installation. When you have gathered the information in these checklists, you can then install Quality Management.

Pre-installation Checklist

Use this checklist to verify the customer’s site meets the requirements for installing Quality Management.

Table 42. Pre-installation checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete Quality Management sizing worksheet</td>
<td></td>
</tr>
<tr>
<td>Verify NIC support for promiscuous mode; recommend driver update if needed</td>
<td></td>
</tr>
<tr>
<td>Verify desktop hardware and disk requirements as defined by the Installation Guide</td>
<td></td>
</tr>
<tr>
<td>Verify there is sufficient disk space. See “Disk Storage Sizing Guidelines” on page 31 for information on estimating the amount of disk storage required for your system.</td>
<td></td>
</tr>
<tr>
<td>Verify system specifications as defined by the Installation Guide</td>
<td></td>
</tr>
</tbody>
</table>
### Pre-order Validation Checklist

Use the following checklist to validate the order before you order Quality Management.

**Table 43.** Pre-order validation checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate customer needs for MetaData/Agent Tagged Calls</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete Quality Management sizing worksheet</td>
<td></td>
</tr>
<tr>
<td>Verify NIC support for promiscuous mode; recommend driver update if needed</td>
<td></td>
</tr>
<tr>
<td>Verify desktop hardware and disk requirements as defined by the <em>Installation Guide</em></td>
<td></td>
</tr>
<tr>
<td>Verify there is sufficient disk space. See “Disk Storage Sizing Guidelines” on page 31 for information on estimating the amount of disk storage required for your system.</td>
<td></td>
</tr>
<tr>
<td>Verify system specifications as defined by the <em>Installation Guide</em></td>
<td></td>
</tr>
<tr>
<td>Evaluate customer needs for MetaData/Agent Tagged Calls</td>
<td></td>
</tr>
</tbody>
</table>
Environment Information Checklist

Use the following checklist to verify the environment information meets requirements.

Table 44. Environment information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CCX version</td>
<td></td>
</tr>
<tr>
<td>Number of agent workstations</td>
<td></td>
</tr>
<tr>
<td>Number of supervisor/managers workstations</td>
<td></td>
</tr>
<tr>
<td>Number of knowledge workers (the non-ACD users that you want to record)</td>
<td></td>
</tr>
<tr>
<td>Number of evaluators</td>
<td></td>
</tr>
</tbody>
</table>

IP Phone Models and Remote Access Checklist

Use the following checklist to verify the IP phone models used at the customer site and verify remote access for deployment resources.

Table 45. IP phone models and remote access checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify IP phone models</td>
<td></td>
</tr>
<tr>
<td>Verify remote access for deployment resources</td>
<td></td>
</tr>
</tbody>
</table>
Base Server Information Checklist

Use the following checklist to gather Quality Management Base Server information.

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Management base server IP address</td>
<td></td>
</tr>
<tr>
<td>Quality Management base server IP hostname</td>
<td></td>
</tr>
<tr>
<td>Quality Management administrator login</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>

Cisco Unified CC Database Checklist

Use the following checklist to gather Cisco Unified CCX information.

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize users with ACD</td>
<td></td>
</tr>
<tr>
<td>Side A Server Name</td>
<td></td>
</tr>
<tr>
<td>Side A IP Address</td>
<td></td>
</tr>
<tr>
<td>Side B Server Name, if one exists</td>
<td></td>
</tr>
<tr>
<td>Side B IP Address, if one exists</td>
<td></td>
</tr>
<tr>
<td>DB Instance Name</td>
<td>rdsaux01_uccx</td>
</tr>
<tr>
<td>Port</td>
<td>1504</td>
</tr>
<tr>
<td>DB Instance Name user login</td>
<td>• Username: uccxworkforce</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>
Cisco Unified CM Information Checklist

Use the following checklist to gather Cisco Unified CM information.

Table 48. Cisco Unified CM information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP AXL user login</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td>JTAPI user login—The same account used for CTI integration</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td>Publisher and Subscribers Host Name/IP Address</td>
<td></td>
</tr>
<tr>
<td>Subscriber IP addresses or hostnames</td>
<td></td>
</tr>
<tr>
<td>Primary CTI Managers</td>
<td></td>
</tr>
<tr>
<td>Backup CTI Managers</td>
<td></td>
</tr>
</tbody>
</table>

SQL Server Checklist

Use the following checklist to order the SQL Server.

Table 49. SQL Server checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order the SQL Server 2005 Standard Edition or SQL Server 2008 Standard Edition</td>
<td></td>
</tr>
</tbody>
</table>
SQL Database Server Information

Use the following checklist to gather Quality Management SQL Database Server information.

Table 50. SQL server information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Management SQL database server IP address or hostname</td>
<td></td>
</tr>
<tr>
<td>Quality Management SQL database server instance name — The default is mssqlserver.</td>
<td></td>
</tr>
<tr>
<td>Quality Management SQL database server login—Default language must be English. Assign the dbowner, dbcreator and dbreader roles to this login.</td>
<td>• Username:&lt;br&gt;• Password:</td>
</tr>
<tr>
<td>User login for remote access (for example, VPN or RDP)</td>
<td>• Username:&lt;br&gt;• Password:&lt;br&gt;• Quality Management system site name:</td>
</tr>
</tbody>
</table>

Quality Management CTI Service Information

Use the following checklist to gather Quality Management CTI service information. The Quality Management CTI service is usually located on the Quality Management server.

Table 51. Enterprise Settings information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Quality Management CTI Service IP address or hostname</td>
<td></td>
</tr>
<tr>
<td>Secondary Quality Management CTI Service IP address or hostname (if any)</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Settings Information Checklist

Use the following checklist to gather Enterprise Settings information.

Table 52. Enterprise Settings information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the Quality Management software licenses</td>
<td></td>
</tr>
</tbody>
</table>

Active Directory Domain Information Checklist

Use the following checklist to gather Active Directory domain information. This information is required only if you use Active Directory with Quality Management.

Table 53. Active Directory domain information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base DN</td>
<td></td>
</tr>
<tr>
<td>Domain name</td>
<td></td>
</tr>
<tr>
<td>Active Directory IP address or hostname</td>
<td></td>
</tr>
<tr>
<td>Port number for AD connection (default is 389 or 636 if you are using SSL)</td>
<td></td>
</tr>
</tbody>
</table>
| Active Directory display name (Created for Read Only)—This user may reside in a different OU than the Quality Management users | • Username:  
  • Password: |
| User Search Base                       |                             |
| Location of the CA certificate for AD  |                             |
Recording File Storage Information Checklist

Use the following checklist to gather Quality Management recording file storage information.

**Table 54.** Recording file storage information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User records—Containers in the Active Directory tree used to locate and link Active Directory users to Quality Management users. A path or paths to user record, and organizational unit records. Quality Management requires this information is only when using Active directory accounts for Quality Management user authentication.</td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
</tbody>
</table>

**Quality Management Server Environment**

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Management Voice/Screen Recording Server IP address or hostname</td>
<td>Provide the storage location (for example, C:\Program Files\Common Files\QM\Recordings)</td>
</tr>
<tr>
<td>If you chose an external storage location, provide the username and password required to access that location</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>
Monitoring and Notification Information Checklist

Use the following checklist to gather monitoring and notification information.

Table 55. Monitoring and notification information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you chose SNMP notification, provide the necessary configuration information (for example, IP addresses for SNMP trap)</td>
<td></td>
</tr>
<tr>
<td>If you chose email notification, provide the necessary configuration information</td>
<td>• IP address or hostname (for example, <a href="mailto:exchange@example.com">exchange@example.com</a>):</td>
</tr>
<tr>
<td></td>
<td>• Port number:</td>
</tr>
<tr>
<td></td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td>• From address:</td>
</tr>
<tr>
<td></td>
<td>• Emergency address:</td>
</tr>
</tbody>
</table>

Remote User Information Checklist

Use the following checklist to gather remote user information.

Table 56. Remote user information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User login for remote access (for example, VPN or RDP)</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td>• Quality Management system site name:</td>
</tr>
</tbody>
</table>
RTP Filters Information Checklist

Use the following checklist to gather information on RTP filters.

Table 57. Remote user information checklist

<table>
<thead>
<tr>
<th>Quality Management Server Environment</th>
<th>Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP filter IP addresses or port addresses</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td>• Site name for Quality Management:</td>
</tr>
</tbody>
</table>

Deployment Activities

Deploying Quality Management is a three-day activity. The following topics describes the activities for each day.

Day 1

The following list describes activities for day 1.

TASK
1. Connect to the customer’s production servers.
2. Verify all server connections are successful based on the information provided in the pre-installation checklist.

ADDITIONAL INFORMATION: See “Pre-Installation Checklists” on page 159 for more information.
3. Gather Active Directory information, if required.

Day 2

The following list describes activities for day 2.

TASK
1. Validate Active Directory information, if required.
2. Install Quality Management from the installation DVD.
3. Complete the Site Configuration Setup tool.

4. Link all contact center agents to their respective Active Directory account, if Active Directory is used.

5. Create an MSI to push Quality Management Administrator, Calabrio Screen Player Plug-in, and Desktop Recording service out to user workstations, prepare to install the client applications at each user’s workstation.

6. Stop site configuration tasks at server and create first evaluation form.

**ADDITI0NAL INFORMATION:** The evaluation form is required for the system setup. Ask the customer to modify and return the sample evaluation form based on business processes for Desktop Recording service. Review and modify it, if needed.

7. Continue site configuration.

8. Meet with the customer to confirm the final configuration based on the customer’s business processes. Ask any questions before completing the site configuration. Confirm workflows and then complete the installation based on answers provided by the customer.

**STEP RESULT:** You should complete site’s configuration by the end of the day.

9. Place test calls to agent workstations, and check for recordings.

10. Test the Upload On Demand feature.

---

**Day 3**

The following list describes activities for day 3.

**TASK**

- Verify the agent recordings were uploaded from the previous day and use the evaluation form to check calls.

- Verify the global upload time settings are consistent with the agent daily log on/log off activity.
Installation Checklists

Use the installation checklists when installing and configuring Quality Management.

Deployment Information Checklist

Use this checklist to gather deployment information.

Table 58. Deployment information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned installation date</td>
<td></td>
</tr>
<tr>
<td>Deployment engineer</td>
<td></td>
</tr>
<tr>
<td>Site address</td>
<td></td>
</tr>
<tr>
<td>Primary contact phone</td>
<td></td>
</tr>
<tr>
<td>Primary contact email address</td>
<td></td>
</tr>
</tbody>
</table>

Server Information Checklist

Use this checklist to gather Quality Management Server information when installing Quality Management.

Table 59. Server information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Management database user login</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td>Verify DNS resolution of IP address and hostname for Quality Management Server on corporate network</td>
<td></td>
</tr>
</tbody>
</table>
**Active Directory Information Checklist**

Use this checklist to gather Active Directory information when installing Quality Management.

*Table 60.* Active Directory information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td></td>
</tr>
<tr>
<td>Base DN</td>
<td></td>
</tr>
</tbody>
</table>
| Active Directory user login |  • Username:  
                              |  • Password:          |

**Unified CM Information Checklist**

Use this checklist to gather Unified CM information when installing Quality Management.

*Table 61.* Unified CM information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
</tbody>
</table>
| Unified CCX                            |  • Username:  
                              |  • Password:          |
| JTAPI user login                       |  • Username:  
                              |  • Password:          |
| AXL user login                         |  • Username:  
                              |  • Password:          |
| Remote access method (Cisco VPN, SSL VPN) |                        |
| Remote access user login               |  • Username:  
                              |  • Password:          |
### Build Server Information Checklist

Use this checklist to gather build server information when installing Quality Management.

**Table 62.** Build server information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Microsoft SQL Server 2005 Standard Edition or SQL Server 2008 Standard Edition (including database, workstation components, Books Online, and development tools) and select the Mixed Mode option in the Authentication Mode screen</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Create an SQL user account, select English as the default language, and select dbcreator from the list of server roles</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Clear Enforce Policy option</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Set Server Roles to dbcreator</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Set SQL collation to Latin1_General</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Add Windows Firewall exclusions by application (if Windows Firewall or other firewall utility is active)</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Allow remote connections</td>
<td>![Insert image here]</td>
</tr>
<tr>
<td>Configure the SQL Server Browser</td>
<td>![Insert image here]</td>
</tr>
</tbody>
</table>

### Optional: Install Windows SNMP Services Checklist

Use this checklist when installing Windows SNMP services.

**Table 63.** Install Windows SNMP services checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Windows SNMP services (optional)</td>
<td>![Insert image here]</td>
</tr>
</tbody>
</table>
Services Installation Checklist

Use this checklist when installing services for Quality Management.

Table 64. Services installation checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the setup_MonRec_802.exe and all selected services shown in the dialog will be installed to the server</td>
<td></td>
</tr>
</tbody>
</table>

Initial Mode Configuration Checklist

Use this checklist to record information when the Site Configuration Setup runs for the first time.

Table 65. Initial mode configuration checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address for Quality Management Directory Services and services</td>
<td></td>
</tr>
<tr>
<td>Enter password for the Quality Management Administrator and note it on this worksheet</td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco Unified CC Database Checklist

Use this checklist to record information when you enter the Cisco Unified CCX information.

Table 66. Unified CCX database checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Side A Server Name</td>
<td></td>
</tr>
<tr>
<td>Enter Side A IP Address</td>
<td></td>
</tr>
<tr>
<td>Enter Side B Server Name, if one exists</td>
<td></td>
</tr>
<tr>
<td>Enter Side B IP Address, if one exists</td>
<td></td>
</tr>
<tr>
<td>DB Instance Name user login</td>
<td>• Username: uccxworkforce</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>

Cisco Unified CM Checklist

Use this checklist to record information when you enter the Cisco Unified CM information. For each cluster, enter the following information.

Table 67. Cisco Unified CM checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP AXL Access username</td>
<td></td>
</tr>
<tr>
<td>SOAP AXL Access password</td>
<td></td>
</tr>
<tr>
<td>JTAPI username</td>
<td></td>
</tr>
<tr>
<td>JTAPI password</td>
<td></td>
</tr>
<tr>
<td>Unified CM hostname or IP address</td>
<td></td>
</tr>
<tr>
<td>Primary or backup CTI Manager</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address for the subscribers (if any) and Primary or Backup designation</td>
<td></td>
</tr>
</tbody>
</table>
Database Checklist

Use this checklist to record information when you configure the Quality Management database.

Table 68. Database checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Quality Management Database hostname or IP address</td>
<td></td>
</tr>
<tr>
<td>Enter the SQL instance name (Leave blank if you want to use the default instance.)</td>
<td></td>
</tr>
<tr>
<td>Select the Unlimited check box</td>
<td></td>
</tr>
</tbody>
</table>
| Enter the username and password for the Quality Management Database | • Username:  
• Password: |

Quality Management CTI Service Checklist

Use this checklist to record information when you configure the Quality Management CTI service.

Table 69. Quality Management CTI service checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the hostname or IP address for the primary Quality Management CTI service</td>
<td></td>
</tr>
<tr>
<td>Enter the hostname or IP address for the backup Quality Management CTI service</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Settings Checklist

Use this checklist to record information when you configure the Quality Management CTI service.

Table 70. Enterprise settings checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Enable Automatic Updates for All Quality Management Clients check box</td>
<td></td>
</tr>
<tr>
<td>Configure session time-outs for Cisco Unified Workforce Optimization and Quality Management Administrator</td>
<td></td>
</tr>
<tr>
<td>View license information and update software licenses by importing a new software license file</td>
<td>Location of the Quality Management software licenses, if not obtained from CVD:</td>
</tr>
<tr>
<td>Configure Active Directory domains (in an Active Directory system only)</td>
<td></td>
</tr>
<tr>
<td>Enable/disable non-English locales (in a system with non-English versions of Quality Management installed)</td>
<td></td>
</tr>
</tbody>
</table>
Optional: Domain Information Checklist

Use this checklist to record information when you configure the domain information.

Table 71. Domain information checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Base DN</td>
<td></td>
</tr>
<tr>
<td>Enter the domain name</td>
<td></td>
</tr>
<tr>
<td>Enter the hostname or IP address</td>
<td></td>
</tr>
<tr>
<td>Enter the port number</td>
<td></td>
</tr>
<tr>
<td>Enter the Active Directory display name</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td>• User Search Base:</td>
</tr>
<tr>
<td>Select the Use SSL check box if Secure Socket Layer is enabled</td>
<td></td>
</tr>
<tr>
<td>Enter the user records (OUs)</td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
<tr>
<td></td>
<td>• OU:</td>
</tr>
</tbody>
</table>
# Recording File Storage Location Checklist

Use this checklist to record information when you configure the recording file storage location.

**Table 72.** Recording file storage location checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address for the voice recordings storage location</td>
<td></td>
</tr>
<tr>
<td>Choose Local Storage Location or External Storage Location for the voice</td>
<td></td>
</tr>
<tr>
<td>recording storage location</td>
<td></td>
</tr>
<tr>
<td>Enter the storage location to any local or external folder for the voice</td>
<td></td>
</tr>
<tr>
<td>recording storage location</td>
<td></td>
</tr>
<tr>
<td>Enter the IP address for the screen recording storage location</td>
<td></td>
</tr>
<tr>
<td>Select the Use Same Path as Voice Recordings check box to store screen recordings</td>
<td></td>
</tr>
<tr>
<td>in the same location as the voice recordings</td>
<td></td>
</tr>
<tr>
<td>If you selected External Storage Location, enter the username and password.</td>
<td>• Username:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>

# Upload Settings Checklist

Use this checklist to record information when you configure the recording file upload settings.

**Table 73.** Upload settings checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Peak Uploads hour parameters</td>
<td></td>
</tr>
<tr>
<td>Enter Off Peak Uploads hour</td>
<td></td>
</tr>
<tr>
<td>parameters</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring and Notification Checklist

Use this checklist to record information when you configure monitoring and notification.

Table 74. Monitoring and notification checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Use Monitoring/Notification Service</td>
<td></td>
</tr>
<tr>
<td>Select Use Event View Notification if required and configure SMTP options</td>
<td></td>
</tr>
<tr>
<td>Select notification triggers</td>
<td></td>
</tr>
</tbody>
</table>

RTP Filters Checklist

Use this checklist to record information when you configure the RTP Filters.

Table 75. Monitoring and notification checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAD ports</td>
<td></td>
</tr>
<tr>
<td>CAD Recording server</td>
<td></td>
</tr>
<tr>
<td>Identify additional RTP filters by IP address or port</td>
<td></td>
</tr>
</tbody>
</table>

Status Checklist

Use this checklist to verify the version of Quality Management.

Table 76. Status checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the information on the screen is correct</td>
<td></td>
</tr>
</tbody>
</table>
Checklists and Activities
Installation Checklists

Install JTAPI Checklist

Use this checklist to record the information when you install JTAPI.

Table 77. Install JTAPI checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Quality Management Administrator Sync Service to run as local user account that is shared with Unified CCX</td>
<td></td>
</tr>
</tbody>
</table>

Quality Management Checklist

Use this checklist to verify all Quality Management are running and verify connections.

Table 78. Quality Management checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the Quality Management Base Server</td>
<td></td>
</tr>
<tr>
<td>Start Quality Management Sync Service</td>
<td></td>
</tr>
<tr>
<td>Verify the FCSS0021 Log Entry</td>
<td></td>
</tr>
</tbody>
</table>

Screen Recording Gateway Checklist

Use this checklist when you configure Screen Recording Gateway. This checklist applies only to systems that include screen recording.

Table 79. Screen Recording Gateway checklist

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Screen Recording Gateway permissions for administrators</td>
<td></td>
</tr>
</tbody>
</table>
### Client Applications Checklist

Use this checklist when installing client applications for Quality Management.

**Table 80. Client applications checklist**

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Quality Management Administrator—http://&lt;base services IP address&gt;:8088/TUP/QM/Administrator.htm</td>
<td></td>
</tr>
<tr>
<td>Install the Calabrio Screen Player Plug-in for managers and supervisors (and agent, if required by the customer)—http://&lt;base services IP address&gt;:8088/TUP/QM/Desktop.htm</td>
<td></td>
</tr>
<tr>
<td>Install the Desktop Recording service—http://&lt;base services IP address&gt;:8088/TUP/QM/Recording.htm</td>
<td></td>
</tr>
<tr>
<td>Verify login for Quality Management Administrator and Cisco Unified Workforce Optimization, if allowed</td>
<td></td>
</tr>
</tbody>
</table>

### Quality Management Administrator Checklist

Use this checklist when configuring Quality Management Administrator.

**Table 81. Quality Management Administrator checklist**

<table>
<thead>
<tr>
<th>Deployment Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the Inclusion List</td>
<td></td>
</tr>
<tr>
<td>Use the wild cards “?” and “*” to configure ranges of extensions</td>
<td></td>
</tr>
<tr>
<td>Select Inbound and/or Outbound check boxes to limit recordings to calls going in a specific direction</td>
<td></td>
</tr>
<tr>
<td>Enable Evaluation for managers and supervisors</td>
<td></td>
</tr>
<tr>
<td>Deployment Task</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Link AD to ACD Users</td>
<td></td>
</tr>
<tr>
<td>Create Quality Management users for non-agent roles</td>
<td></td>
</tr>
<tr>
<td>Assign roles to Quality Management users</td>
<td></td>
</tr>
<tr>
<td>License users</td>
<td></td>
</tr>
<tr>
<td>Assign Quality Management supervisors to ACD teams</td>
<td></td>
</tr>
<tr>
<td>Create groups</td>
<td></td>
</tr>
<tr>
<td>Assign teams to groups</td>
<td></td>
</tr>
<tr>
<td>Assign managers to groups</td>
<td></td>
</tr>
<tr>
<td>Configure recording retention periods</td>
<td></td>
</tr>
<tr>
<td>Configure training retention period</td>
<td></td>
</tr>
<tr>
<td>Configure agent tagged retention period</td>
<td></td>
</tr>
<tr>
<td>Enter archive recording retention period or select Unlimited</td>
<td></td>
</tr>
<tr>
<td>Select Allow Agents to Access Archive, if allowed</td>
<td></td>
</tr>
<tr>
<td>Create evaluation forms</td>
<td></td>
</tr>
<tr>
<td>Configure who can evaluate contacts that use a specific form</td>
<td></td>
</tr>
<tr>
<td>Configure who can approve evaluation that use a specific form</td>
<td></td>
</tr>
<tr>
<td>Create an archive workflow per customer requirements</td>
<td></td>
</tr>
<tr>
<td>Create an archive workflow per customer requirements</td>
<td></td>
</tr>
<tr>
<td>Add user-defined metadata elements</td>
<td></td>
</tr>
<tr>
<td>Deployment Task</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Enable or disable recording export at the role level per customer requirements</td>
<td></td>
</tr>
</tbody>
</table>
Backup and Restore

There are two situations when you need to create a backup of Quality Management data.

• Upgrading your system to the latest version of Quality Management
• Making a disaster recovery backup for Quality Management data

Upgrades

When upgrading from version 2.6, or version 2.7 to version 8.5, the installation process automatically backs up your data and restores it to the newly-installed version 8.5. It is not necessary to manually backup and restore the data.

Disaster Recovery

Use the Backup and Restore features available in the Microsoft SQL Server Management Studio to back up and restore Quality Management version 8.5 databases.

The SQMDB database stores historical data and report data.

Backup the databases to a folder on the computer that hosts the Microsoft SQL Server 2005.

NOTE: After you back up the Quality Management database, it is advisable to copy the backup files to another location for safekeeping.

Back up the Quality Management Databases

Use this task to back up your Quality Management system.

Task

1. Open Microsoft SQL Server Management Studio (choose Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio).

2. Right-click the database name (SQMDB) under the Databases node.

Step Result: A menu appears.

**STEP RESULT:** The Restore Database window appears.

4. Complete the fields and click OK.

---

**Restoring the Quality Management Database**

Use this task when you need to restore your Quality Management system from the backup files due to a database corruption or some other problem.

**TASK**


2. Stop the following services for Quality Management:
   - DB Cleaner service
   - DB Proxy service
   - Mana service
   - Sync service
   - Upload Controller service
   - Network Recording service
   - Monitor service
   - Jetty on the Voice and Screen server and the Base server

   
   a. Right-click the database name (SQMDB) under the Databases node.
      
      **RESULT:** A menu appears.
   
   b. Choose Tasks > Restore > Database.
      
      **RESULT:** The Restore Database window appears.
   
   c. Complete the fields and click OK.

4. Restart the services for Quality Management you stopped in Step 2.
Index

A
Active Directory 61, 98
  configuration guidelines 61
  domain name 62
automated package distribution tools 69
  best practices 71
  requirements 69
Automated Update feature 95

B
backup 185
  backup and restore 185

C
Calabrio Screen Player Plug-in 13
CDR information formats 116
Choose Monitor Adaptor 131
Cisco Unified CC database 82
Cisco Unified CCX database 82
Cisco Unified CM 86
Cisco Unified Workforce Optimization 14
  client applications 13, 66
  components 13
Configure Local Services 131
Create Database Catalogs 131
CTI Manager 86
CTI service 14, 90

D
data configuration environment 19
DB Cleaner service 14
Desktop Recording service
  about 14
  network interface cards (NICs) 43

E
phone configurations 44
  requirements 42
  disaster recovery 185
  Display Metadata Encryption Key 131
  Download /Install JTAPI 131

F
email addresses 112
Encrypt Audio Files 131
enterprise settings 93

G
firewall requirements 45

H
hardware VPN 33

I
ignored extensions 120
Initial Mode 73
installation order 13
installation status 127
IP phones
  supported 35
  tested 36
J
Jetty service 15
L
license 96
importing 97
licensing rules 98
license type 16
licensing
rules 98
Live Monitor
considerations 40
M
Mana service 15
Microsoft SQL server 52
Monitor service 15
monitoring and notification 108
Monitoring and Recording database 81
N
network interface cards (NICs) 43
Network Recording
considerations 37
Network Recording service 15
notification triggers 115
NT Authentication 135
upgrade guidelines 142
O
operating environment 20
P
PostInstall.exe 73
Q
Quality Management Administrator 13
R
Real-time Transport Protocol (RTP)
filters 123
guidelines 124
recording file storage location 102, 103
recording requirements 37
remote agent
supported configurations 32
Remove Recording 131
removing Monitoring and Recording 155
removing QM 151
restore 185
retention periods 141
S
server capacity guidelines 26
Server Recording
considerations 37
services 14
session timeout options 95
Set Recording Home Directory 131
single server configuration 17
Site Configuration Setup 73
Site Configuration Setup tools 130
SMTP settings 113
SNMP settings 111
software updates 95
software VPN 32
Start Local Services 131
Sync service 15
system requirements 18
T
Test CTO Service(s) 131
third-party applications 34
U
Update Mode 73
upgrade status 127
upgrades
backup and restore 185
guidelines 142
Monitoring and Recording 143, 144
Upload Controller service 15
upload settings 106
W
web applications 14
web browser
considerations 35
Windows SNMP services 59
workflows 141