Release Notes for Cisco Workforce Optimization Quality Management Release 2.3(1)

Revised: December 4, 2007

These release notes describe the new features for Cisco Workforce Optimization Quality Management Release 2.3(1).

Use these release notes in conjunction with the Quality Management 2.3 documentation.

Contents

These release notes discuss the following topics:

System Requirements

Quality Management 2.3(1) is compatible with the following Cisco Unified Contact Center environments:

Unified CCX Version	Unified CM Version
4.1(n)	4.3
5.0(n)	5.1, 6.0

New and Changed Information

This is the first release for Quality Management.

Limitations and Workarounds

A Service Release Must Be Removed Manually When Performing a Major Version Upgrade

Symptom: Service release is not removed, and no messages are displayed when attempting to upgrade both client and server software.

Description: During an upgrade, the installer does not check to see if any service releases have been applied.

Workaround: In Control Panel, start the Add or Remove Programs utility and verify that no service releases are present. QM service releases are listed as "Quality Management Service Release". If there are service releases, remove them before attempting an upgrade.

Quality Management Recordings Exceed Upload Limits Set in QM Administrator

Symptom: An agent uploads more Quality Management recordings in one day than is configured in the Number Recordings/Agent/Day field on the Workflow Administration > Workflow window in QM Administrator.

Description: Agents using multiple PCs in a single day may upload more Quality Management recordings than the number specified in the Number Recordings/Agent/Day field.

Workaround. Have the agent use only one PC per day.

Stopping QM CTI Service During Calls May Corrupt JTAPI User

Symptom: The JTAPI user becomes inaccessible when the QM CTI Service restarts.

Description: Stopping the QM CTI Service on the QM CTI server machine may corrupt the JTAPI user on the Cisco Unified CM. This has been seen intermittently on Cisco Unified CM 5.0.

Workaround:

Step 1   In Cisco Unified CM, delete the existing JTAPI user.

Step 2   Create a new JTAPI user and associate all phone devices with that user.

Step 3   In QM Administrator, enter the new JTAPI username and password on the Site Configuration > CallManager Clusters window.

Step 4   Restart the QM CTI service.

Unable to Retrieve Active Directory (AD) Users

Symptom: QM Administrator cannot retrieve AD users when linking AD users to ACD users.

Description: Users that are configured in AD without a first or last name cannot be retrieved by QM.

Workaround: Ensure that all AD users are configured with a first name, last name, and display name.

CSV Reports Do Not Open in Microsoft Internet Explorer 7

Symptom: When attempting to save reports in CSV format, a dialog to save appears but disappears very quickly.

Description: The dialog appears and disappears so quickly that you cannot save the reports to CSV format.

Workaround:

Step 1   Double-click **My Computer**.

Step 2   Choose **Tools > Folder Options**, and select the **File Types** tab.

Step 3   Under Registered File Types, select **XLS Microsoft Excel Worksheet**, and then click **Advanced**.

Step 4   Clear the **Confirm open after download** check box, and then click **OK**.

Request to Close Application Appears During an Automatic Update

Symptom: A message appears during automatic client upgrades asking the user to close the application before continuing.

Description: Automatic update fails to close the applications automatically, so it asks for the user to do it.

Workaround: Click **Ignore** and the process continues. This message may appear multiple times.

RTP Codec G.722 is Not Supported

Symptom: Recordings are 1KB in length.

Description: If voice recordings are 1KB long, no RTP traffic is being recorded. The recording client filters out any codecs it does not support.

Workaround: Configure the phone device so that it does not use the G.722 codec.

Open Caveats

The following issues are open in QM 2.3(1).

Note You can view more information and track individual QM defects using the Cisco Bug Toolkit located at:
http://www.cisco.com/support/bugtools/Bug_root.html

Table 1   Open caveats in release 2.3(1).

Identifier	Severity	Headline
CSCsi98597	2	Exception on voice file closing causes subsequent recordings to be lost
CSCsi98421	3	Recording files stranded in Staging folder after reboot
CSCsi98491	3	Install process does not check for SR installs on client or server
CSCsi98545	3	AD Linking: Shows error when AD server reaches max search result limit
CSCsi98560	3	Upload processing gets stuck in "Already Processing" loop
CSCsi98577	3	Calls with same filename created after recovery to LDAP
CSCsi98583	3	Reports--Generic msg for when browser session times out
CSCsi98590	3	Blank spaces are allowed when creating new user
CSCsi98595	3	Uploads get stuck in "Invalid handle" loop

Documentation Revisions

This section describes the changes made to Quality Management 2.3 documentation after its release.

Quality Management Service Information Manual

Date Revised: November 4, 2007

Page Number: 132

Original Text: **Problem**: The client application installations do not download when the links on the installation web page are clicked.

Symptom: When the install program link is clicked, a "HTTP 404—File Not Found" error is displayed.

Cause: QM Site Configuration was not completed successfully on the Base services server.

Solution: On the QM Base services server, start QM Configuration Setup. In Windows Explorer, navigate to the C:\Program Files\Cisco\WFO_QM\bin folder and double-click **PostInstall.exe**.

If Configuration Setup starts in Initial Mode, it was not completed correctly. Go through each window and make sure that all required data is entered, and then click **Finish**.

If Configuration Setup starts in Update Mode, start QM Configuration Setup. From the menu bar, choose **File > Reset Client Installs**. This places the client install files in the default location, and reconfigures them to use the default setting for the IP address of the LDAP server.

Try to install the client applications from the installation web page again. If the problem persists, contact technical support.

Updated Text: **Problem**: The client application installations do not download when the links on the installation web page are clicked.

Symptom: When the install program link is clicked, an "HTTP 404–File Not Found" error is displayed.

Cause: QM Site Configuration was not completed successfully on the Base services server.

Solution: On the QM Base services server, do the following:

1. Navigate to the C:\Program Files\Cisco\WFO_QM\bin folder and double-click **PostInstall.exe** to start QM Configuration Setup.

2. From the **Tools** menu, choose **Generate Info for MSI Clients**. This will recreate the MSI files that are opened from the links on the installation web page.

3. Navigate to the C:\Program Files\Cisco\WFO_QM\Tomcat\webapps\TUP\QM folder and verify that there are three MSI files in the folder:

   - Cisco Unified WFO Quality Management Administrator.msi
   - Cisco Unified WFO Quality Management Desktop.msi
   - Cisco Unified WFO Quality Management Recording.msi

If the files are not there, and if the QM Base server is running Windows 2003 Server, do the following steps:

1. Open a command window and navigate to the C:\Program Files\Cisco\WFO_QM folder.

2. Type the following commands, pressing **Enter** after each line:

```
.\bin\transform.bat 1033
cd bin
piupdate <QM Base services server IP address>
```

3. Navigate to the C:\Program Files\Cisco\WFO_QM\Tomcat\webapps\TUP\QM folder and verify that there are three MSI files in the folder:

   - Cisco Unified WFO Quality Management Administrator.msi
   - Cisco Unified WFO Quality Management Desktop.msi
   - Cisco Unified WFO Quality Management Recording.msi

Quality Management Installation Guide

Date Revised: December 4, 2007

Page Number: 14

Original Text: In Table 4, "Supported Desktop Component Operating Systems and Hardware," a supported operating system is listed as:

Windows XP Professional, Service Pack 1 or later

Updated Text: Change this to:

Windows XP Professional, Service Pack 2 or later

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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