Release Notes for Cisco Unified Communications Manager Business Edition 5000 Release 8.6(1a)

August 23, 2011

To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL:

http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html

Table 1 Updates to Release Notes for Cisco Unified Communications Manager 8.6(1a) Release Notes

Date	Changes
06/24/11	Updated the following sections for Cisco Unified Communications Manager information for Release 8.6(1a): • Introduction, page 2 • System Requirements, page 2 • Upgrading to Unified CM 8.6(1a), page 3 • Related Documentation, page 21 • Limitations and Restrictions, page 21 • Important Notes, page 21 • Caveats, page 33 • Documentation Updates, page 46
08/23/11	Added CSCtr62446 Route List Run on All Nodes Service Parameter, page 33.

Contents

This document includes the following information:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Before you install or upgrade Cisco Unified Communications Manager (Unified CM), Cisco recommends that you review the "Upgrading to Unified CM 8.6(1a)" section on page 3, and the "Latest Software and Firmware Upgrades for Unified CM 8.6 on Cisco.com" section on page 20 for information pertinent to installing or upgrading, and the "Important Notes" section on page 21 for information about issues that may affect your system.

Introduction

Unified CM, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

Cisco Unified Communications Manager Business Edition 5000 (Unified CMBE) offers you the features and functionality of Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection on one appliance platform.

Note In the past, export licenses, government regulations, and import restrictions have limited Cisco System's ability to supply Unified CM worldwide. Cisco has obtained an unrestricted US export classification for Unified CM.

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not even allowed to fresh install a restricted version on a system that contains an unrestricted version.

System Requirements

The following sections provide the system requirements for this release of Unified CM.

Server Support

Make sure that you install and configure Unified CM on a Cisco Media Convergence Server (MCS), a Cisco Unified Computing System (UCS) server, or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS and UCS servers are compatible with this release of Unified CM, refer to the Supported Servers for Unified CM Releases: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.

Note Make sure that the matrix shows that your server model supports Unified CM Release 8.6(1a).

Note Be aware that some servers that are listed in the *Cisco Unified Communications Manager Software Compatibility Matrix* may require additional hardware support for Unified CM Release 8.6(1a). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Uninterruptible Power Supply (UPS) Integration for Unified CM

Cisco recommends that you connect each Unified CM server to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

Integration occurs via a single point-to-point USB connection. Serial and SNMP connectivity to UPS is not supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported with the APC SmartUPS 1500VA USB and APC 750VA XL USB. The feature activates automatically during bootup if a connected UPS is detected.

Alternatively, you can execute the CLI command **show ups status** that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started. The CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime, and other relevant status information.

When the feature is activated, graceful shutdown will commence as soon as the low battery threshold is reached. Resumption or fluctuation of power will not interrupt or abort the shutdown, and administrators cannot stop the shutdown after the feature is activated.

For unsupported Unified CM releases, MCS models or UPS models, you can cause an external script to monitor the UPS. When low battery is detected, you can log in to Unified CM by using Secure Shell (SSH), access the CLI, and execute the **utils system shutdown** command.

Note If your pre-8.0 Unified CM runs on a deprecated server, you can upgrade it by using the Bridge upgrade procedure.

Note Be aware that the DL 380-G6 server is available only directly from HP; no equivalent HP OEM MCS-7835-H3 or MCS-7845-H3 servers exist.

Upgrading to Unified CM 8.6(1a)

The following sections contain information that is pertinent to upgrading to this release of Unified CM.

- Software Version Number, page 4
- Pre-Upgrade Tasks, page 4
- Software Upgrade Considerations, page 6
- Obtaining the Upgrade File, page 9
- Ordering the Upgrade Media, page 9
- Software Upgrade Procedures, page 10
- Post-Upgrade Tasks, page 17
- Installing COP Files, Dial Plans, and Locales, page 19

- Latest Software and Firmware Upgrades for Unified CM 8.6 on Cisco.com, page 20
- CSCtr11072 Music On Hold Audio File Upload May Be Slow Or May Fail To Upload, page 22

Caution When you upgrade to Cisco Unified Communications Manager 8.6(1a), the system reboots several times as part of the upgrade process and the service outage period is longer than with traditional upgrades. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

Caution If you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software. Note that IP phone security configurations will be modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Note For Unified CM 8.6(1a), a non-bootable image is available for download from Cisco.com. This image may be downloaded to a network server (remote source) or burned to DVD (local source) and used for upgrades. Unified CM 8.6(1a) DVDs ordered from Cisco are bootable and may be used for fresh installs.

Caution Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Software Version Number

These release notes are based on following software versions:

- Unified CM: 8.6.1.20000-1

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks: For Cisco Unified Communications Manager Business Edition 5000, the release notes are located at

http://cisco.com/en/US/products/ps7273/prod_release_notes_list.html

- Ensure that you have the necessary license files for the new release.

  For more information on obtaining and installing licenses, see the License File Upload chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Before you begin the upgrade, back up your system. This is particularly important if you are upgrading software on HP7825H3 or HP7828H3 hardware as there is no option to revert to the previous version.

- If you are upgrading software on HP7825H3 or HP7828H3 hardware, ensure that you have a 16GB USB device available to migrate your data to the new system. For Unity Connection and Business Edition 5000, a 128GB external USB device is required. It is recommended to use an externally powered USB drive as other drives may not be recognized during the Refresh Upgrade sequence.
- Disable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Note Be aware that, when you deactivate the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

Caution Failure to deactivate the Cisco Extension Mobility service could cause the upgrade to fail.

- Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.
- Before you upgrade to a later release, refer to the documentation for your currently installed COP files to identify any special considerations related to upgrading Cisco Unified Communications Manager.

Note If you have the Nokia s60 COP file installed, you must install any newer version of it before you upgrade Cisco Unified Communications Manager.

- If you plan to use IPv6 with Cisco Unified Communications Manager Release 8.0(2) or later, you can provision your DNS server for IPv6 prior to upgrading to Release 8.0(2) or later. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you perform the upgrade.

Caution Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.0(2) or later causes the upgrade to fail.

- Before you upgrade a cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (publisher server) and subsequent nodes (subscriber servers). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.
- Before you perform the Cisco Unified Communications Manager upgrade, ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.
- After you complete the pre-upgrade tasks, review with the "Software Upgrade Considerations" section on page 6.

Software Upgrade Considerations

This section contains the following topics:

- Overview of the Software Upgrade Process, page 6
- Making Configuration Changes During an Upgrade, page 7

Overview of the Software Upgrade Process

You cannot install upgrade software on your server while the system continues to operate.

Caution If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use an externally powered 16GB USB device to facilitate data migration from the old system to the new installation. For Unity Connection and Business Edition 5000, a 128GB external USB device is required. It is recommended to use an externally powered USB drive as other drives may not be recognized during the Refresh Upgrade sequence.

When you install 8.6 upgrade software, there will be a temporary server outage while the CUCM software is installed. Once you kick off the upgrade using either the command line or graphical user interface the data will be exported, and the system will be automatically rebooted at which point the server outage will begin. The duration of this outage will depend on your configuration and amount of data. During the upgrade, progress can be monitored via the console until such time that command line interface and graphical user interface access has been restored. Once restored, you can use the command line interface or graphical user interface to continue to monitor upgrade progress.

Note If an administrator or a phone user makes changes during the upgrade process (export of data), that data could be lost after upgrade.

When you initiate the upgrade, you can indicate to activate the partition with the new upgrade software or return to using the partition with the previous version of the software at upgrade completion. With the exception of HP 7825H3 and HP7828H3 hardware upgrades, the previous software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since you upgraded the software will get lost.

Note You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

You can upgrade from a DVD (local source) or from a network location (remote source) that the Cisco Unified Communications Manager Business Edition 5000 server can access.

For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings changes made by phone users might get unset. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

Caution Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Upgrading to Unified CM 8.6(1a) on a Virtual Server

If you run Cisco Unified Communications Manager on a virtual server, and are upgrading to the 8.6.1 release, you must make sure that the virtual server's Guest Operating System and RAM meet the requirements for the latest release.

To upgrade Cisco Unified Communications Manager on a virtual server, do the following:

Step 1 Upgrade the virtual machine to the latest release. For information on installing or upgrading Cisco Unified Communications Manager on virtual servers, refer to the document *Cisco Unified Communications Manager on Virtualized Servers.*

Step 2 After you finish the upgrade, shut down the virtual machine.

Step 3 Change the Guest Operating System to **Red-Hat Enterprise Linux 5 (32-bit).**

Step 4 Check the RAM on the virtual machine and make sure that it meets the minimum RAM requirements for this release. Refer to the readme file that accompanied this release's OVA file for minimum RAM requirements at: **Products\Voice and Unified Communications\IP Telephony\Call Control\Cisco Unified Communications Manager (CallManager)\Cisco Unified Communications Manager Version 8.6\Unified Communications Manager Virtual Machine Templates**.

Step 5 Save changes.

Step 6 Restart the virtual machine.

Making Configuration Changes During an Upgrade

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration Changes

The administrator must not make any configuration changes to Cisco Unified Communications Manager during an upgrade. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option windows.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

If you are upgrading your system, you must complete the upgrade tasks in this section before you perform any configuration tasks.

Caution If you fail to follow these recommendations, unexpected behavior may occur; for example, ports may not initialize as expected.

Upgrade Tasks

To successfully complete the upgrade, perform the upgrade tasks in the following order before you begin making configuration changes.

Note Cisco strongly recommends that you do not perform configuration tasks until the upgrade completes on all servers in the cluster, until you have switched the servers over to the upgraded partition, and until you have verified that database replication is functioning.

Procedure

Step 1 Stop all configuration tasks; that is, do not perform configuration tasks in the various Cisco Unified Communications Manager-related GUIs or the CLI (with the exception of performing the upgrade in the Cisco Unified Communications Operating System GUI).

Step 2 Upgrade the first node in the cluster (the publisher node).

Note The switch version for the publisher will occur in step 4. However, if upgrading from Unified CM 8.5 or earlier, choose to run new version at the completion of the upgrade; step 4 is not required.

Step 3 Upgrade the subsequent nodes in the cluster (the subscriber nodes).

Note The switch version for subscribers will occur in step 5. However, if upgrading from Unified CM 8.5 or earlier, choose to run new version at the completion of the upgrade; step 5 is not required.

Step 4 Switch over the first node to the upgraded partition.

Step 5 Switch over subsequent nodes to the upgraded partition.

Note You can switch the subsequent nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 6 Ensure that database replication is functioning between the first node and the subsequent nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified CM Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:

- 0— Initializing.
- 1—Replication setup script fired from this node.
- 2—Good replication.
- 3—Bad replication.
- 4—Replication setup did not succeed.

Before you proceed, ensure that you have a good database replication status. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 7 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

User Provisioning

For upgrades from Cisco Unified Communications Manager Release 8.x, changes that are made to the following user-facing features get preserved after the upgrade completes:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication
- Recording enabling
- Single Number Reach enabling

Obtaining the Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com. You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Ordering the Upgrade Media

To upgrade to Unified CM Release 8.6(1a) from a release prior to 8.0(1), use the Product Upgrade Tool (PUT) to obtain a media kit and license or purchase the upgrade from Cisco Sales.

To use the PUT, you must enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD/DVD set. If you do not have a contract for Unified CM, you must purchase the upgrade from Cisco Sales.

For more information about supported Unified CM upgrades, see the *Cisco Unified Communications Manager Software Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

See the "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide*.

Software Upgrade Procedures

This section provides procedures for upgrading from either a local or a remote source and contains the following topics:

- Upgrading Software or Installing Locales from a Local Source, page 11
- Upgrading Software or Installing Locales from a Remote Source, page 13

Installing the COP File

Caution For both restricted and unrestricted upgrades from an 8.5(x) or earlier release to an 8.6(x) release, this patch (COP file) must be applied prior to initiating the upgrade. Before you upgrade from compatible versions of Unified CM, install the COP file named **ciscocm.refresh_upgrade_v1.1.cop.sgn** that you can find under:

Cisco Unified Communications Manager Version 8.6>Unified Communications Manager / CallManager / Cisco Unity Connection Utilities>COP-Files

Upgrading to Restricted or Unrestricted Unified CM 8.6(1a)

If upgrading from 8.5(1) or earlier complete the"Installing the COP File" section on page 10.

Note The unrestricted version of Unified CM 8.6(1a) is available in limited markets only.

Be aware that after you install or upgrade to an unrestricted release, you can never upgrade to a restricted version. You are not even allowed to fresh install a restricted version on a system that contains an unrestricted version

Upgrading from Unified CM 6.x or Later by Using the UCSInstall ISO File

Note Release 6.x and 7.x customers can upgrade to this version, but the Cisco CallManager service will not run unless an 8.0 Software Feature License exists on the system.

Procedure

Step 1 From the Software Download page on Cisco.com, download the appropriate UCSInstall iso file.

For the restricted version:
UCSInstall_UCOS_8.6.1.20000-1.sgn.iso

For the unrestricted version:
UCSInstall_UCOS__UNRST_8.6.1.20000-1.sgn.iso

Note Because the UCSInstall_UCOS_8.6.1.20000-1 build specifies a nonbootable ISO, the build proves useful only for upgrades. You cannot use this build for new installations.

Step 2 Use an md5sum utility to verify the MD5 sum of the final file.

For the restricted version:

```
1fffdad07be38d63bb64a29b821f0e0f UCSInstall_UCOS_8.6.1.20000-1.sgn.iso
```

For the unrestricted version:

```
f5fb68b8d99b0335bd1013eb1dad73e4 UCSInstall_UCOS_UNRST_8.6.1.20000-1.sgn.iso
```

Upgrading Software or Installing Locales from a Local Source

To upgrade the software from local DVD, follow this procedure:

Procedure

Step 1 If upgrading from 8.5(1) or earlier complete the“Installing the COP File” section on page 10.

Step 2 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Unity Connection and Business Edition 5000, a 128GB external USB device is required.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Step 3 If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to Step 4.

If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:

- **a.** Start Cisco Unity Connection Serviceability.
- **b.** Navigate to **Tools > Control Center - Feature Services**.
- **c.** Under Critical Services, in the Connection Conversation Manager row, click **Stop**.
- **d.** Wait for the service to stop.
- **e.** Also under Critical Services, in the Connection Mixer row, click **Stop**.
- **f.** Wait for the service to stop.

Step 4 Insert the new DVD into the disc drive on the local server that is to be upgraded.

Step 5 Log in to Cisco Unified Communications Operating System Administration.

Step 6 Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 7 From the **Source** list, choose **DVD**.

Step 8 Enter a slash (/) in the Directory field.

Step 9 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 10 To continue the upgrade process, click **Next**.

Step 11 Choose the upgrade version that you want to install and click **Next**.

Step 12 In the next window, monitor the progress of the download.

Step 13 If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to Step 14.

If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to Step 6.

If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:

a. Start Cisco Unity Connection Serviceability.

b. Navigate to **Tools > Control Center - Feature Services**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.

d. Wait for the service to start.

e. Also under Critical Services, in the Connection Mixer row, click **Start**.

f. Wait for the service to start.

g. Skip the rest of the procedure.

Step 14 If you want to run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager and you will not be able to choose **Switch to new version after upgrade**.

Step 15 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps, choose **Do not switch to new version after upgrade**.

Step 16 Click **Next**. Depending on your configuration, the following text appears:

a. For non-HP7825H3/HP7828H3 hardware:
A Refresh Upgrade requires that the server be rebooted during the upgrade. Services will be affected during the upgrade operation. Press OK to proceed with the upgrade.

b. For HP7825H3/HP7828H3 hardware:
This server model requires a USB storage device in order to proceed with the upgrade. Please insert a USB storage device with at least 16GBytes of capacity. Note that any existing data on the USB device will be deleted.

Note For Unity Connection and Business Edition the USB storage device must be 128 GBytes.

The Upgrade Status window displays the Upgrade log.

Step 17 When the installation completes, click **Finish** (not applicable for Refresh Upgrades).

Step 18 To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software (not applicable for Refresh Upgrades).

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Supported SFTP Servers

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Cisco does not support using the SFTP product free FTDP. This is because of the 1GB file size limit on this SFTP product.

For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

Upgrading Software or Installing Locales from a Remote Source

To upgrade the software from a network location or remote server, use the following procedure.

Note Do not use the browser controls, such as Refresh/Reload, while you are accessing Cisco Unified Communications Operating System Administration. Instead, use the navigation controls that are provided by the interface.

Procedure

Step 1 If upgrading from 8.5(1) or earlier complete the“Installing the COP File” section on page 10.

Step 2 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation. For Unity Connection and Business Edition 5000, a 128GB external USB device is required.

Step 3 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

Step 4 If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to Step 5.

If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:

a. Start Cisco Unity Connection Serviceability.

b. Navigate to **Tools > Control Center - Feature Services**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.

d. Wait for the service to stop.

e. Also under Critical Services, in the Connection Mixer row, click **Stop**.

f. Wait for the service to stop.

Step 5 Log in to Cisco Unified Communications Operating System Administration.

Step 6 Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 7 From the **Source** list, choose **Remote Filesystem**.

Step 8 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 9 In the **Server** field, enter the server name or IP address.

Step 10 In the **User Name** field, enter your user name on the remote server.

Step 11 In the **User Password** field, enter your password on the remote server.

Step 12 Select the transfer protocol from the **Transfer Protocol** field.

Step 13 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 14 To continue the upgrade process, click **Next**.

Step 15 Choose the upgrade version that you want to install and click **Next**.

Step 16 In the next window, monitor the progress of the download.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again:

Warning: Another session is installing software, click Assume Control to take over the installation.

If you are sure you want to take over the session, click **Assume Control**.

If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 17 If you are installing upgrade software, skip to Step 18.

If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to Step 6.

If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:

a. Start Cisco Unity Connection Serviceability.

b. Navigate to **Tools > Control Center - Feature Services**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.

d. Wait for the service to start.

e. Also under Critical Services, in the Connection Mixer row, click **Start**.

f. Wait for the service to start.

g. Skip the rest of the procedure.

Step 18 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.

Step 19 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps, choose **Do not switch to new version after upgrade**.

Step 20 Click **Next**. Depending on your configuration, the following text appears:

a. For non- HP7825H3/HP7828H3 hardware:
A Refresh Upgrade requires that the server be rebooted during the upgrade. Services will be affected during the upgrade operation. Press OK to proceed with the upgrade.

b. For HP7825H3/HP7828H3 hardware:
This server model requires a USB storage device in order to proceed with the upgrade. Please insert a USB storage device with at least 16GBytes of capacity. Note that any existing data on the USB device will be deleted.

Note For Unity Connection and Business Edition the USB storage device must be 128 GBytes.

The Upgrade Status window displays the Upgrade log.

Step 21 When the installation completes, click **Finish** (not applicable for Refresh Upgrades).

Step 22 To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software (not applicable for Refresh Upgrades).

Bridge Upgrade

The bridge upgrade provides a migration path for customers who want to migrate from discontinued Cisco Unified Communications Manager server to a server that supports the newest release of Cisco Unified Communications Manager.

Servers that are no longer supported, but are permitted to function as bridge upgrade servers, can upgrade and boot but will not allow Cisco Unified Communications Manager to function.

When you attempt to upgrade your Cisco Unified Communications Manager version on a discontinued server model, Cisco Unified Communications Manager inserts a message into the upgrade log. The upgrade log is displayed on the web browser when the upgrade is initiated through the Cisco Unified Communications Operating System Administration window, or you can view it through CLI if you used CLI to perform the upgrade. This message notes that you can only use the new version to obtain a DRS backup. The warning message in the log is followed by a delay that allows you to cancel the upgrade if you do not want to do a bridge upgrade.

When the system boots the new Cisco Unified Communications Manager version, a warning appears on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality."). Because of the restricted visibility of the console, the warning displays during both CLI and GUI sessions.

Use the following procedure to perform a bridge upgrade:

Procedure

Step 1 Perform an upgrade to the new Cisco Unified Communications Manager version on your discontinued first node (publisher) server. Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do. Observe the warning on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup ("This hardware has limited functionality. Backup and Restore is the only supported functionality.").

Step 2 Perform an upgrade to the new Cisco Unified Communications Manager version on your subsequent node (subscriber) servers. Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do.

Step 3 Verify database synchronization between all nodes. You can use the CLI commands utils dbreplication runtime state and utils dbreplication status. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 4 Using the new Cisco Unified Communications Manager version on your discontinued first node server, perform a DRS backup. The DRS backups are encrypted using the cluster security password provided at install time. You must remember this security password as the "old" password, because you may be prompted to enter this "old" password at the time of restore. Refer to the *Disaster Recovery System Administration Guide*.

Step 5 Disconnect your discontinued server from the network.

Step 6 Install the new Cisco Unified Communications Manager version on your new supported first node server. You must obtain and install a new license on this server. Refer to the guide *Installing Cisco Unified Communications Manager*. You will be prompted to enter a "new" security password, a password that is different from the "old" password you noted in Step 4. The guide *Installing Cisco Unified Communications Manager* describes the requirements of a "new" security password that Cisco Unified Communications Manager will accept. You must remember this "new" security password.

Step 7 Using the new Cisco Unified Communications Manager version on your new supported first node server, perform the *Disaster Recovery System Administration Guide* procedure "Restoring the First Node only (Rebuilding the Publisher Alone)". First, select only select the first node for restore. You can only select the subsequent nodes for restore after the completion of first node restore. Use the discontinued server's backup file that you created in Step 4. You will be prompted for the "old" security password that you noted in Step 4. For further details, refer to the *Disaster Recovery System Administration Guide*.

Step 8 On your new supported first node server, reactivate all services that used to be active on your discontinued first node server before the bridge upgrade. Refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Step 9 Verify database synchronization between all nodes. You can use the CLI commands utils dbreplication runtime state and utils dbreplication status. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Post-Upgrade Tasks

After the upgrade, perform the following tasks:

- Enable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

  Note If you do not enable the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line
- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
  - Do Not Disturb

  - Privacy
  - Presence
  - CTI call control
  - Busy Lamp Field
- If necessary, reinstall the Real Time Monitoring Tool.

Reverting to a Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by using the Switch Version option to switch the system to the software version on the inactive partition.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://*server-name***/cmplatform**

where *server-name* specifies the host name or IP address of the Cisco Unified Communications Manager Business Edition 5000 server.

Step 2 Enter your Administrator user name and password.

Step 3 Choose **Settings > Version**.

The Version Settings window displays.

Step 4 Click the **Switch Versions** button.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 To verify that the version switch was successful, you can follow these steps:

a. Log in to Open Cisco Unified Communications Operating System Administration again.

b. Choose **Settings > Version**.

The Version Settings window displays.

c. Verify that the correct product version is now running on the active partition.

d. Verify that all activated services are running.

e. For the publisher node, log in to Cisco Unified Communications Manager Administration by entering the following URL and entering your user name and password:

https://*server-name***/ccmadmin**

f. Verify that you can log in and that your configuration data exists.

Installing COP Files, Dial Plans, and Locales

This section contains the following topics:

- COP File Installation, page 19
- Dial Plan Installation, page 19
- Locale Installation, page 19

COP File Installation

The following guidelines apply to installing COP files. If the documentation for a specific COP file contradicts these general guidelines, follow the COP file documentation:

- Install the COP file on every server in a cluster.
- After you install a COP file, you must restart the server.

Note You must restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database. Cisco recommends that you perform this restart during an off-peak period.

Dial Plan Installation

You can install dial plan files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the "" section on page 11 for more information about this process.

After you install the dial plan files on the system, log in to Cisco Unified Communications Manager Administration and then navigate to **Call Routing > Dial Plan Installer** to complete installing the dial plans.

Locale Installation

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

User Locales

User locale files provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. User-only locale installers exist on the web.

Network Locales

Network locale files provide country-specific phone tones and gateway tones, if available. Network-only locale installers exist on the web.

Cisco may combine multiple network locales in a single locale installer.

Cisco Unity Connection Locales

Cisco Unity Connection locales (languages) provide country-specific system prompts, graphical user interface, and text-to-speech functionality. For information on downloading Cisco Unity Connection locales, see the "Installation and Upgrade Information" section of the applicable Cisco Unified Communications Manager Business Edition 5000 release notes at http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html.

Caution Do not install more than five Cisco Unity Connection locales.

Installing Locales

You can install locale files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the "" section on page 11 for more information about this process.

Note To activate the newly installed locales, you must restart the server.

See the "Cisco Unified Communications Manager Locale Files" section on page 20 for information on the Cisco Unified Communications Manager locale files that you must install. You can install more than one locale before you restart the server.

Cisco Unified Communications Manager Locale Files

When you are installing Cisco Unified Communications Manager locales, you must install the following files:

- User Locale files—Contain language information for a specific language and country and use the following convention:

  cm-locale-*language*-*country*-*version*.cop

- Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

  cm-locale-combinednetworklocale-*version*.cop

Latest Software and Firmware Upgrades for Unified CM 8.6 on Cisco.com

After you install or upgrade to this release of Unified CM, check to see if Cisco has released software upgrades, firmware upgrades, critical patches or Service Updates.

Firmware

Applying the latest comprehensive Firmware Upgrade CD (FWUCD) can prevent catastrophic failures and should be applied as soon as possible.

To check for the latest FWUCD from www.Cisco.com:

- select **Support > Download Software**

- Navigate to **Products > Voice and Unified Communications > Communications Infrastructure > Voice Servers > Cisco 7800 Series Media Convergence Servers (or Cisco UCS B-Series Blade Servers) > *(your server model).***

Software

Service Updates (SUs), contain fixes that were unavailable at the time of the original release. They often include security fixes, firmware updates, or software fixes that could improve operation.

To check for software upgrades, Service Updates, critical patches, from www.Cisco.com:

- select **Support > Download Software**
- Navigate to the "Voice and Unified Communications" section and select **IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager) >** ***the appropriate version of Cisco Communications Manager for your deployment***.

Related Documentation

You can view documentation that supports this release of Unified CM at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

For information about the Cisco Intercompany Media Engine server, see the Release Notes for Cisco Intercompany Media Engine Release 8.6(1a) at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_6_1/rel_notes/ime-rel_notes-861.html.

Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Unified CM System testing. The recommendations, which are not exclusive, represent an addition to interoperability recommendations for each individual voice application or voice infrastructure product.

For a list of software and firmware versions of IP telephony components and contact center components that were tested for interoperability with Unified CM 8.6(1a) as part of Cisco Unified Communications System Release 8.x testing, see the following web page:

http://www.cisco.com/go/unified-techinfo

Note Be aware that the release of Cisco IP telephony products does not always coincide with Unified CM releases. If a product does not meet the compatibility testing requirements with Unified CM, you need to wait until a compatible version of the product becomes available before you can upgrade to Unified CM Release 8.6(1a). For the most current compatibility combinations and defects that are associated with other Unified CM products, refer to the documentation that is associated with those products.

Important Notes

The following section contains important information that may have been unavailable upon the initial release of documentation that supports Unified CM Release 8.6(1a).

- CSCtr11072 Music On Hold Audio File Upload May Be Slow Or May Fail To Upload, page 22

CSCtr11072 Music On Hold Audio File Upload May Be Slow Or May Fail To Upload

Music On Hold audio file upload time may be extended or fail to upload. Refresh the browser to view current status. If the file fails to upload after 30 minutes, reduce the file size.

CSCtq96181 Cannot Add or Edit H323 Gateway on Device/Gateway Web Page

In Unified CM 8.6.1 version 8.6.1.10000-43, the H.323 Gateway Configuration web page has missing field labels and does not allow configuration of data.

There are 2 ways to resolve this issue:

- Apply the COP file ciscocm.gatewayH323.cop.sgn, available here:

  Cisco Unified Communications Manager Version 8.6>Unified Communications Manager/CallManager/Cisco Unity Connection Utilities>COP-Files
- Upgrade to Unified CM 8.6(1a) version 8.6.1.20000-1

Note The administrator must logout and log back in for the COP file changes to take effect.

Unrestricted Release Limitations

After you install an unrestricted release, you can never upgrade to a restricted version. You will not even be allowed to fresh install a restricted version on a system that contains an unrestricted version.

New in User Options Page Beta

The User Option Page Beta provides a first look at a redesign concept for the User Option pages. The intent is to simplify the user experience by making the User Option Pages easier to learn and use.

Features Covered in the User Options Page Beta:

- Reach Me Anywhere
- Call Forwarding
- Speed Dials
- Password Management
- Pin Management

How to access the User Option Page Beta

The User Option Page Beta can be accessed at:

https://[UCM_HOSTNAME]:8443/ucmuser

The classic User Option Pages can still be accessed at:

https://[UCM_HOSTNAME]:8443/cucmuser

Limitations and Caveats with User Option Page Beta

- Not all user options are configurable (see Features Covered above)
- User must associated with phone in UCM administration
- The associated phone must have a line configured
- Only one user phone will be managed via the User Option Page Beta (phone that is users primary line)
- User must be associated with a remote destination profile
- End User must be in the Standard End User Group

CSCtq56727 SIP Gateway Crash During Heavy Call Traffic

A SIP gateway crash occurs during heavy call traffic when the Unified CM SIP trunk is configured with DTMF signaling type as “no preference” and the SIP gateway is configured with dtmf relay as “sip-kpml”.

To resolve this issue, set the CCM SIP trunk DTMF signaling type as “OOB and RFC 2833” and reload the gateway router.

CSCtq78686 - CoRes RU failure from 6.1.4.2000-2 to 8.6.1.10000-42

Upgrading from 6.1.4 to 8.6 (RU) may fail due to importing the 'iproduct' library in CAR export script. This failure is rare.

While RU, exportcardb.py runs to export the records present in CAR DB. In this script there is an import statement like 'import iproduct' which is required for further processing. When the system tries to import this module, it can't find the module named 'iproduct' and produces the following error:

```
06/02/2011 17:48:44 component_install|(CAPTURE)     import iproduct|<LVL::Debug>

06/02/2011 17:48:44 component_install|(CAPTURE) ImportError: No module named
    iproduct|<LVL::Debug>
```

Unity Connection (UC) delivers a different version of python than the active side normally uses (i.e. the active side is v2.2 and UC uses v2.4). Unity adds their "bin" area at the head of the PATH variable causing UC’s version of python to be implemented, causing /usr/lib/python2.2 to setup with iproduct, ihardware and other modules normally used for processing. Since the exportcardb.py script is calling /usr/bin/env python as part of the #! line, it is picking up the wrong version of python to run and there is no library setup for that version of python (UC didn't setup anything).

To resolve this issue, complete the following procedure. To avoid this issue altogether, perform steps 1 and 2.

Procedure

Step 1 Perform a step by step upgrade from Unified CM software version 6.1.4 to latest 7.x.

Step 2 Perform a step by step upgrade from Unified CM software version latest 7.x to 8.6(1).

Step 3 Upgrade again (second attempt) from Unified CM software version 6.1.4 to 8.6(1) directly.

CSCtq84756 MCS 7835/45-I3 Server Freezes During Firmware Upgrade

When upgrading uEFI firmware version 1.07 to version 1.08 or later on a 7835/45-I3 server, the server freezes after system reboot. This occurs due to a bug in uEFI firmware version 1.07 which prevents the server from acquiring the new firmware during system reboot.

To resolve this issue, press "F3" during reboot to force the server to acquire the new firmware update. Alternatively, a complete AC power cycle may be required.

CSCtq47285 RingOut State Transfer or Hold

In all versions of Cisco Unified Communications Manager, when a call is in RingOut state, you cannot transfer it or put it on hold.

Verify RAID Status Prior To Upgrade on 7825H3 and 7828H3 Servers

Note Prior to an L2 upgrade, execute the following CLI command to ensure that test-raid has passed:

```
utils diagnose module raid
```

Note Prior to an L2 upgrade, execute the following CLI command to ensure that Rebuild Status is not displayed.

```
show hardware
```

CSCtq46578 iso file download error message

When an iso file is downloaded as part of an upgrade, there are a number of safeguards which occur. The following need to be highlighted:

- The first, which technically occurs before the file is downloaded, is to confirm that the file name of the file matches expected heuristics and rules of the upgrade. This heuristic and upgrade rules check can be executed remotely.
- A cryptographic digest of the downloaded iso file contents is then created and presented to the user in order to confirm the file's accuracy according to the Cisco web site. This process analyzes the contents of the iso, not the iso file itself, therefore the iso file must be mounted in order for the user to access its contents. The cryptographic digest process must be run locally on the server. If the iso file is corrupted, the cryptographic digest flags the iso as unusable and the operating system displays the following error message:

```
Buffer I/O error on device loop0, logical block
```

These messages are normal, and there are numerous reasons why a downloaded iso file may be corrupted: premature disconnection of the downloading client, inadequate amount of storage on the client or temporary network issues. If any of these download issues occur, download the iso file again from Cisco once the network, server, or other issue has been resolved.

CSCto31364 Cluster Fully Qualified Domain Name (CFQDN) Parameter

The Cluster Fully Qualified Domain Name (CFQDN) parameter in the Clusterwide Domain Configuration section of the Cisco Unified Communications Manager Enterprise Parameters (System > Enterprise Parameters) must either be blank or configured so that it does not match the hostname of any of the Cisco Unified MeetingPlace nodes. If a match occurs, SIP REFER will not function properly because the call will not be routed by a SIP route pattern.

CSCto83868 firmware update error message

When a 7845I3 or 7835I3 server (running ServeRaid MR10i firmware older than 11.0.1.-0033) is booted from a Unified CM 8.6(1a) installation DVD during a fresh installation, the following error message occurs:

```
Firmware update failing from 11.0.1.-0024
```

Select “continue”. The server will continue installing normally. When the server boots from the hard disk during the 2nd phase of the installation, the firmware is successfully updated.

CSCtd87058 BAT Impact

If your Unified CM is unrestricted, Cisco recommends that you do not edit the following fields by using BAT - Import/Export:

- Configuring a Phone Security Profile - Device Security Mode field. Default specifies Non Secure
- Cisco IOS Conference Bridge Configuration Settings - Device Security Mode field. Default specifies Not Selected.
- Configuring Voice Mail Port Wizard - Device Security Mode field. Default value specifies Not Selected.
- Configuring Voice Mail Port - Device Security Mode field. Default specifies Not Selected
- Configuring SIP Trunk Security Profile - Device Security Mode field. Default specifies Non Secure.

Cisco Unified Communications Manager Business Edition Name Change

Beginning with release 8.5(1), Cisco Unified Communications Manager Business Edition gets renamed Cisco Unified Communications Manager Business Edition 5000.

Call Park Feature Limitations

The Call Park feature has the following known limitations:

- CSCsz18443 Cisco Unified IP Phone 8961, 9951, 9971 Registered to a Node may Use the Call Park Number Assigned to Another Node, page 26
- CSCsz31137 Parked Call Gets Reverted When the Parkee is on, page 27
- CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve, page 27
- CSCtb53159 Display Limitation in ConfList, page 27

CSCsz18443 Cisco Unified IP Phone 8961, 9951, 9971 Registered to a Node may Use the Call Park Number Assigned to Another Node

Call Park numbers get configured on the nodes of a Unified CM cluster (first/subsequent). Call Park numbers are normally allocated from the node that initiates the call. If the Cisco Unified IP Phone 8961, 9951, 9971 that initiates the call is registered to the first node of the Unified CM cluster, then a Call Park number configured on the first node gets used to park the call. This is irrespective of the node to which the called party is registered, or which party (calling or called) invokes the Call Park feature.

For example, if a phone registered to the first node initiates a call to a phone registered to the second node, then regardless of which phone invokes the Call Park feature, a Call Park number configured on the first node is always used.

Similarly, if the Call Park feature gets invoked when a phone in the second node is the call initiator, then a Call Park number configured on the second node is used.

Note Be aware that you can restrict the Call Park feature only by using calling search space and partitions. Not configuring a Call Park number on a node will not ensure that the Call Park feature is not available to the phones in that node.

CSCsz31137 Parked Call Gets Reverted When the Parkee is on

When an inter-cluster parked call connected by an Intercluster Trunk (ICT) is put on hold, the call reverts when the Park Monitoring Reversion Timer and the Park Monitoring Forward No Retrieve Timer expire. Such a call reverts even though the parkee is on hold. This is a known limitation of inter-cluster calls connected via ICT that use the Call Park feature.

CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve

For inter-cluster parked called connected by an ICT, after the Park Reversion Timer and Park Monitoring Forward No Retrieve Timer expire, the call gets forwarded to the Park Monitoring Forward No Retrieve destination. The display of the incoming call is incorrect on the destination device.

The display on the device is “From DN” instead of “Forwarded for DN”. For example, if the initial call is an inter-cluster call via ICT from DN 1000 to DN 3000 and gets forwarded to DN 2000, the display on DN 2000 is “From 3000" instead of “Forwarded for 1000".

CSCtb53159 Display Limitation in ConfList

You can add as many conference participants as the conference bridge supports; however, ConfList only displays 16 participants. From the 17th participant onwards, the list displays only the latest 16 participants.

CSCth53322 Rebuild Server After You Use the Recovery Disk

After you use the recovery disk to bring a server with a corrupted file system into a bootable and semi-functional state, Cisco recommends that you rebuild the server.

Note If you do not rebuild the server, you may notice missing directories, lost permissions, or corrupted softlinks.

CSCte05285 IBM I3 Servers Automatic Server Restart (ASR) Default Specifies Disabled

In the event of a system lockup, IBM I3 type servers do not automatically restart.

Under rare critical failures, such as a kernel panic, the IBM I3 type platforms do not automatically get restarted by the BIOS ASR functionality. The server remains unresponsive until it is rebooted manually.

Condition

In **IMM Control > System Settings > Server Timeouts**, the OS Watchdog timeout default specifies disabled.

Workaround

Before you perform the workaround make sure that the following conditions exist:

- Cisco Unified CM install is complete and the system is operational
- IMM remote management web interface is configured. (For details on how to configure IMM, refer to the hardware documentation.)

Procedure

To change the OS Watchdog configuration setting:

1. Log into the IMM remote management web interface.
2. From **IMM Control > System Settings > Server Timeouts**, change the OS Watchdog timeout value to **04:00**. This configures the timeout to 4 minutes.

Caution Do not configure any other timeout duration.

CSCtd01766 Destination Port on Trunk Remains Unchanged After Upgrade

During an upgrade to an unrestricted Cisco Unified CM release, the SIP trunk incoming port gets changed to 5060; however, the destination port on the trunk remains what it was before the upgrade.

CSCtl23382 Recovery CD Issues

You can use the Recovery Disk to try to recover a system when a system is completely unrecoverable in all other ways.

When you boot the server from the Recovery Disk, the options that are summarized in Table 2 display:

Table 2 Recovery Disk Menu Options

[S]|[s]	Swap the active and inactive partitions. This option only appears if a valid inactive partition exists.
[C]|[c]	Clean the system to bare metal state (see Note).
[F]|[f]	Check and automatically correct disk file systems.
[V]|[v]	Verify the disk partitioning layout.

[Q]|[q]	Quit this recovery disk program.

Note The "C" option replaces the "W"option, and performs the same task that "W" used to perform — it cleans out data from the hard disks to prepare the system for Windows installation. The "C" option is especially useful for customers who have 7825/28-H3 servers running with SWRAID in Release 8.6. These customers can perform a fresh install of any version of pre-8.6 Release Cisco Unified Communications Manager by booting their systems with the 8.6 version of the Recovery Disk, and then selecting the "C" option to clean all data from the system.

To use the Recovery Disk, perform the following procedure:

Procedure

Step 1 Insert the Recovery Disk and restart the system so that it boots from the DVD. Once the server completes the boot sequence, the Recovery menu displays.

Step 2 Select the appropriate option from Table 2 on page 28.

Step 3 Select the “Q” option to quit the Recovery Disk program.

Disaster Recovery System Caution

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to re-configure the DRS backup device and schedule.

When you restore your data, the hostname, server IP address, and the deployment type must be the same as it was during the backup. DRS does not restore across different hostnames, IP addresses and products or product suites installed (Cisco Unified Call Manager, Cisco Unified Connection, Cisco Unified Communications Manager Business Edition 5000, etc).

EMCC Login Affects Settings in Product-Specific Configuration Layout of Phone Configuration Window

When a user uses a phone in a visiting cluster to log into the user Extension Mobility profile, the phone inherits the default provisioning, network, and security settings (specifically, the configuration in the Product Specific Configuration Layout section of the Phone Configuration window) from the home cluster.   This behavior may override local security and network settings that are in place in the visiting cluster. Some of the parameters have firmware defaults that the system administrator cannot change until a fix is provided.

CSCtl47624 No Music On Hold when using ASR 1000

The Cisco Unified Border Element (CUBE) on Aggregation Services Router (ASR) 1000 series may not support one-way streaming of music or announcements by the Cisco Unified Communications Manager Music on Hold (MOH) feature. To work around this limitation, set the CUCM Duplex Streaming Enabled MOH service parameter to “True”.

CSCtq20098 To handle DRS Restore status monitoring in a scenario

When the SSO configurations are restored from the DRS Backup during the DRS Restore process in the following scenario, the administrator cannot see the Final DRS Restore results.

System has SSO Enabled for Cisco Unified Operating System Administration option (Cisco Unified OS Administration, Disaster Recovery System).

Procedure

Step 1 Conduct DRS Backup.

Step 2 Disable SSO for Cisco Unified Operating System Administration option (Cisco Unified OS Administration, Disaster Recovery System).

Step 3 Restore the DRS Backup you conducted in Step 1.

During the DRS Restore process, SSO configurations are restored as part of the PLATFORM component. After the PLATFORM component restore is completed, the DRS Restore status displays an HTTP 500 error and the administrator cannot monitor the DRS Restore status from the GUI. At this stage, the administrator must monitor the DRS Restore status from the CLI by executing the utils disaster_recovery status restore command. After a successful DRS restore, the administrator must reboot the system for the DRS restore changes to take effect.

Note If other options (Cisco Unified CM Administration, Cisco Unified CM User Options, Cisco Unified Data Service, RTMT) with SSO configurations are restored as part of a DRS restore, administrators or users will see an HTTP 500 error when they try to access these SSO-enabled options until the system is rebooted after successful DRS restore.

Limitations with Presentation Sharing when using a Cisco TelePresence MCU

Cisco Unified Communications Manager does not support presentation sharing with the Binary Floor Control Protocol when it is used between Unified CM and a Cisco TelePresence MCU.

Video Conferencing with Cisco Integrated Services Routers Generation 2

Cisco Integrated Services Routers Generation 2 (ISR G2) can be enabled to act as IOS-based conference bridges that support ad hoc and meet-me audio and video conferencing. To enable conferencing, a PVDM3 DSP module must be installed on the ISR G2. The ISR G2 includes the following series:

- Cisco 2900 Series
- Cisco 3900 Series

For ad hoc video conferencing, the ISR G2 router supports up to eight participants. For meet-me video conferencing, support is provided for up to 16 participants. For video conferences, the resolution, bit rate and frame rates vary depending on which video format is used, but the ISR G2 can support a frame rate of up to 30 frames per second, a stream bit rate up to 2 Mb/s, and video resolution of up to 704 x 568 pixels. For a detailed breakdown of the codecs, frame rates, bit rates, and video resolution for each video format, see the document *Configuring Video Conferences and Video Transcoding*.

Within Cisco Unified Communications Manager, the ISR G2 can be configured as one of three conference bridge types:

- Cisco IOS Homogeneous Video Conference Bridge—All the conference participants connect to a conference bridge with phones that support the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants.
- Cisco IOS Heterogeneous Video Conference Bridge—All the conference participants connect to the conference bridge with phones that use different video format attributes. Transcoding and transsizing features are required from the DSP in order to convert the signal from one video format to another.
- Cisco IOS Guaranteed Audio Video Conference Bridge—If DSP resources are limited, you can reserve DSP resources for just the audio conference bridge. The DSP resources for the audio conference bridge are reserved, but video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers are connected to the conference as audio participants.

For more detailed information about video conferencing with ISR G2 routers, see the document *Configuring Video Conferences and Video Transcoding*.

Interoperability with a Cisco TelePresence Video Communications Server

Cisco Unified Communications Manager is interoperable with a Cisco TelePresence Video Communication Server (VCS). To make the two systems compatible, a SIP normalization script must be configured on the trunk that connects Cisco Unified Communications Manager to the VCS. The normalization script adjusts the signaling so that the two products can communicate.

In earlier versions of Cisco Unified Communications Manager, the script had to be manually imported into Cisco Unified Communications Manager, but Release 8.6.1 includes the script in the installation using the script name *vcs-interop*.

Refer to the following sections for details on how to handle upgrades from earlier versions and how to configure VCS interoperability in Release 8.6.1.

- VCS Interoperability Issues for Upgrades to Release 8.6.1, page 32
- Configuring VCS Interoperability in Release 8.6.1, page 32

VCS Interoperability Issues for Upgrades to Release 8.6.1

If you are upgrading to Cisco Unified Communications Manager 8.6.1 from an earlier release, and your previous network included a connection to a Cisco TelePresence Video Communications Server (VCS), the upgrade to 8.6.1 will fail if the name of the SIP normalization script used in your previous release was *vcs-interop.* In this case, you must rename the old script prior to completing the upgrade.

To ensure that the upgrade succeeds, complete the following steps before you upgrade to Release 8.6.1:

Step 1 From Cisco Unified Communications Manager Administration, select **Device > Device Settings > SIP Normalization Script.**

Step 2 In the SIP Normalization Script Configuration window, click **Find** to list all the SIP normalization scripts.

Step 3 Check to see if a script with the precise name *vcs-interop* appears. If a normalization script with this exact name appears, it will create a conflict with the *vcs-interop* script in the latest release. You must rename the old script before proceeding with the upgrade. To rename the script:

- **a.** Click on the script to open the SIP Normalization Script Configuration window.
- **a.** In the Name field, rename the script to anything other than *vcs-interop*. Cisco recommends adding the old release number to the script.
- **b.** Click Reset.

Step 4 Proceed with the upgrade.

After upgrading to 8.6.1, complete Configuring VCS Interoperability in Release 8.6.1, page 32 to configure VCS interoperability in Release 8.6.1.

Configuring VCS Interoperability in Release 8.6.1

After installing or upgrading to Cisco Unified Communications Manager 8.6.1, perform the following steps to configure Cisco Unified Communications Manager to interoperate with a Cisco TelePresence Video Communications Server:

Step 1 In Cisco Unified Communications Manager Administration, select **Device > Device Settings > SIP Profile**.

Step 2 Select the SIP profile for the trunk that connects Cisco Unified Communications Manager to the VCS.

Step 3 On the SIP Profile Configuration window, check the **Use Fully Qualified Domain Name** check box.

Step 4 Click **Save** and **Reset**.

Step 5 In Cisco Unified Communications Manager Administration, select **Device > Trunk.**

Step 6 Select the SIP Trunk that connects Cisco Unified Communications Manager to the VCS.

Step 7 In the Normalization Script area, select **vcs-interop** from the SIP Normalization drop-down menu.

Step 8 Leave the Parameter Name and Parameter Value fields empty. If these fields are already completed, delete the field contents. These fields are not used if the Use Fully Qualified Domain Name check box on the SIP Profile Configuration window is checked.

Step 9 Click **Save** and **Reset**.

Call Detail Record Field Options

The list of Call Detail Record (CDR) field options has been updated to include the following codecs and field values:

- H.264 = 103
- AMR Codec = 97
- AMR-WB Codec = 98

CSCtr62446 Route List Run on All Nodes Service Parameter

When you enable Run on All Nodes at the Route List level, the Route List is active on all the call processing nodes.

New and Changed Information

The *New and Changed Information for Cisco Unified Communications Manager 8.6(1)* provides information about new and changed features for release 8.6(1).

To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/8_6_1/delta/delta.html

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of severity levels 1, 2, and 3.

Caveats describe unexpected behavior on a Cisco Unified Communications server. Severity 1 caveats represent the most serious caveats, severity 2 caveats represent less serious caveats, and severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Unified CM Release 8.6(1a) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://tools.cisco.com/Support/BugToolKit.

Using Bug Toolkit

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 Access the Bug Toolkit, http://tools.cisco.com/Support/BugToolKit.

Step 2 Log in with your Cisco.com user ID and password.

Step 3 If you are looking for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field, and click **Go**.

Tip Click **Help** on the Bug Toolkit page for information about how to search for bugs, create saved searches, create bug groups, and so on.

Open Caveats

Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 describe possible unexpected behaviors in Unified CM Release 8.6(1a), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in the "Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011" section on page 35 to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version Field in the Online Defect Record

When you open the online record for a defect, you will see data in the "First Fixed-in Version" field. The information that displays in this field identifies the list of Unified CM interim versions in which the defect was fixed. These interim versions then get integrated into Unified CM releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1. However, the version information that displays for the Unified CM maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Unified CM release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 8.0(2.40000-x) = Cisco Unified Communications Manager 8.0(2c)
- 7.1(5.10000-x) = Cisco Unified Communications Manager 7.1(5)

- 7.1(3.30000-x) = Cisco Unified Communications Manager 7.1(3b)
- 7.1(3.20000-x) = Cisco Unified Communications Manager 7.1(3a)
- 7.1(3.10000-x) = Cisco Unified Communications Manager 7.1(3)
- 7.1(2.30000-x) = Cisco Unified Communications Manager 7.1(2b)
- 7.1(2.20000-x) = Cisco Unified Communications Manager 7.1(2a)
- 7.1(2.10000-x) = Cisco Unified Communications Manager 7.1(2)

Note Because defect status continually changes, be aware that the "Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011" section on page 35 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "Using Bug Toolkit" section on page 33.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log in to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011

The following table lists open caveats which may cause unexpected behavior (as of June 24, 2011) in Unified CM 8.6(1a).

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011

IDENTIFIER	COMPONENT	HEADLINE
CSCtj95738	database-ids	PMR 81654 database out of memory while syncing certificate table
CSCto77709	cpi-appinstall	Communication to Publisher lost after upgrade was started
CSCto81679	cp-mediacontrol	DTMF not working when MGCP gateway
CSCto84611	cp-supplementaryservices	CCM cores when running External Call Control automation
CSCto75049	cp-sip-station	Device Hold Reversion QED Settings Not Properly Checked
CSCtn97718	tftp	slave tftp server become unresponsive intermittently.
CSCto98215	cp-mediacontrol	MCNTRL-1054:RT-7985-ex90 transfer scenario [RT jitter]
CSCtl04228	cp-mediacontrol	Transfer fails - Unified CM 8 > 8.5.1
CSCtq04681	ccm-serviceability	SCH: Pub and Sub both becomes active during fallback
CSCtq10159	cp-mediacontrol	Unified CM tears down call if second TCS message is received in quick succession

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto68768	cmcti	Cannot control device after Migrate Phone until CTIManager restart
CSCtc87894	cp-mediacontrol	Video: UCM sends sendRecv instead of recvOnly for video call over ICT
CSCto17218	cpi-platform-api	Unable to locate files if folder contains names with special characters
CSCte05285	cpi-os	IBM I3 servers Automatic Server Restart (ASR) not enabled by default
CSCtf37698	cmcti	Incorrect reason code in ExistingCallEvent for supervisor
CSCto70998	cp-mediacontrol	Inter-cluster video call between LS & TB establishes as audio call.
CSCtg79013	security	tvs core when Pub/Sub1 switch back to old load after Sub2 install on new
CSCto71473	cp-mediacontrol	meetMee_wrong_reservation-410
CSCto71704	cp-mediacontrol	call_cannot-be_answered
CSCto71830	cp-sip-station	DeviceApplyConfigResult alarm definition is missing information
CSCth58139	cp-mediacontrol	sRTP:E2E-No Audio after simultaneous resume
CSCtl56249	c pi-os	User Prompt<Abort> on RU with less than minimum of disk on legacy models
CSCtn08912	database-ids	PMR 86128 corrupt syscdr resulting in bogus error 62 and/or 92
CSCtl56932	cpi-os	CORE cimserver on Sub while Pub is in process of Refresh Upgrade
CSCto76495	cp-mediacontrol	TRP wrongly handles DSCP markings for Video calls
CSCto77083	car	Hunt Pilot CFNA and CFB reports are not displaying in CAR
CSCto77125	car	Mismatch of Summary/Detail reports for hunt pilot failed and abandoned calls
CSCti69234	cpi-third-party	Security Issue in OpenSSL
CSCto80322	database-ids	Informix assert fail while running 3-day out of memory stress test
CSCto34641	cp-sip-trunk	Need a method to terminate/re-establish KPML subscription
CSCto68227	cmui	Configure Unassociated SD or BLF SD on Cius phone
CSCtn66109	cmcti	Get intermittent fail with Platform exception on transfer to another HP
CSCto86072	syslog	Cannot configure remote syslog on a subscriber node

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto87483	cp-mediacontrol	Get extra StartReception event after answer from redirect over sip trunk
CSCto88439	cp-mediacontrol	MCNTRL-1524:Bug in Agena Interface triggers unnecessary DTMF pro changes
CSCto88449	cp-mediacontrol	MCNTRL1532:MTPAgenaIF sends MXOffer before MXOffer recvd from SIF50
CSCto91596	cp-sip-trunk	DT: X-cisco-user-agent and server header sent incorrectly in xfer case
CSCto49535	cp-supplementaryservices	Call is not cleared from the line on phones by race condition of Pickup
CSCtn71568	cpi-os	Console login sometime doesnt works on Sub
CSCto94478	ims	No warning message when enabling SSO w/o importing OpenAM server cert
CSCtl74581	tapisdk	Mediariver w/ SRTP does not work on 64Bit client
CSCto02728	cmui	Unified CM web very slow for phone queries
CSCto95129	tapisdk	no CONFERENCED call state (IDLE) on Target in app on cBarge
CSCto51280	cp-callcontrol	Two G729 calls consume 160kbp of location bandwidth
CSCto51306	cmui	Slow Admin on Device Search by Device Pool
CSCtk32432	cpi-third-party	Update TPL OpenSSL to Addresss Published Vulnerabilities
CSCto96586	cp-sip-trunk	No audio after blind transfer when SIP SP does not support UPDATE
CSCto96924	cp-mediacontrol	E2E hold-resume video call results in audio call for resumed connection
CSCto72113	cpi-appinstall	uc86-gb-sol
CSCto99391	ccm-serviceability	SCH: Passed-time messages are not sent in the fail over scenarios
CSCto57127	cp-mediacontrol	e2e: hairpin call between EX-90 & RT phone has no video
CSCto57427	cpi-os	Cannot ping ipv6 addresses outside its own subnet from 8.6 Unified CM
CSCtq00323	ccm-serviceability	SNMP agent needs to filter processnodeservice CNs
CSCtn50334	cpi-appinstall	Applying refresh_upgrade COP file after canceled RU gives wrong prompt
CSCto57934	cp-mediacontrol	DTMF sent by the caller does not reach the callee.
CSCtg93134	ccm-serviceability	utils system restart cli command gives error
CSCti81686	cp-mediacontrol	CUBE Does not update the Media Info from ACK/SDP followed by PRACK/SDP
CSCtn00989	cmui	CCMAdmin shows registration unknown after Android registered

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq01514	cp-sip-trunk	Additional Characters in SDI logs when a call made via QSIG SIP Trunk
CSCtq01756	cpi-os	Update NSS RPMs per RHSA-2011:0472-1
CSCto09866	cmcti	Unable to create conference chain with conference bridge
CSCtq04067	cp-sip-station	“Unknown Number” is displayed when "Auto Pickup" is enabled
CSCtq05761	cp-mediacontrol	Blind conferencing over H.323 and SIP EO fails
CSCtn82607	database	PMR 89829 CCM 8.6.0.96071-5: Error 403 during cdr check w/ verbose
CSCtn90839	cuc-tomcat	Adjust Tomcat memory diagnostic to take into account free memory
CSCtq06789	cp-sip-station	“findDeviceByX509Subject: No Entry Found” lines filling the Unified CM traces
CSCtn84005	cp-mediacontrol	h245 session gets stuck after sending the ECS
CSCto62290	cp-sip-station	ApplyConfig does not work when SIP Profile is changed on vsrious RT phones.
CSCto62450	cp-mediacontrol	Attended Xfer of conference over H.323 trunk fails
CSCtq07868	cp-mediacontrol	No MOH for sRTP MGCP FXS endpoint when placed on hold
CSCto11698	database-ids	PMR 00006 data is not replicating between all nodes in cluster some
CSCtq07935	sw-phone-sip	Blind beginEndTransfer failed (phone 2 “ringout” was not cleared)
CSCtq08137	sdl	outgoing connections network trace can crash application
CSCtl44984	database-ids	PMR 84728 Assert Failure yield_processor: Conditional latch count non-ze
CSCtl44987	database-ids	PMR 84726 Assert Failure Fatal Error In Buffer Manager
CSCtq09875	axl	Get License Capabilities failed with UserID having Apostrophe
CSCto17792	cpi-appinstall	Cisco Unity Connection error code ignored by platform during refresh upgrade
CSCtq10460	jtapisdk	Fail to get hunt connection when tranfer to another hunt pilot
CSCtn86264	cpi-os	IBM cimlistener process crashed unexpectedly
CSCtl88901	cpi-os	usb_key_detect core during RU from 6.1.5.10000-7 to 8.6.0.94000-88
CSCto52689	axl	Language not localized in directory page
CSCto71448	cpi-service-mgr	After CUCM upgrade few services operational status remains down

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto82031	cmui	Login error message provides too much information
CSCtq19020	database-ids	PMR 04791 Assert duriXng out of memory testing on 55GB virtual server
CSCtq72623	cp-system	Code yellow under mobile agent NailUp load
CSCtq14129	cp-system	CCM Cored After upgrade to 8.5.1.12018-1
CSCtq70875	backup-restore	CUCM,CUCMBE3000 8.6 - Manual backup job cancellation doesnt terminate.
CSCtq74604	ime-server	IME - Calls to a site who disables IME often fail
CSCtq75780	cp-huntlist	RouteList control not returning - CcRejInd back to correct Cdcc
CSCtq37605	cp-sccp	Lines could not register after SdlLinkOOS
CSCtq41333	cp-sccp	Route list prefix shows up at the caller phone
CSCtq75566	ims	Single Sign On cant be enabled on Unity Connection
CSCtq70900	cpi-cert-mgmt	Tomcat and/or IPSEC Key store corruption causes DRF backup failures
CSCtq55418	cp-mlpp	Receiving Phone always gets Routine MLPP instead of Priority, Flash etc
CSCtq63440	smdiservice	Error reported on console during bootup for usbserial and pl2303 modules
CSCtq67098	cp-digit-analysis	CUCM crashes when LD number is dialed for Germany country pack
CSCtq36661	ext-mobility	HEB: Extension Mobility Menu show up in English for Hebrew Locale
CSCtq37634	cp-device-manager	Lines could not register after SdlLinkOOS
CSCtq40657	cp-qsig	Issue with QSIG over SIP. MWI relay to ISDN PRI QSIG trunk failing
CSCtq22979	rtmt	RTMT login issue when Cisco DB is down
CSCtq76930	risdc	8.6.1.96000-11 mo_main (VIPR) Build Status Is FAILED
CSCtq76428	cp-sip-station	UCM cores when sip station parses corrupt XML in SIPNotifyInd signal
CSCtq43535	cp-sip-trunk	"c=" SDP line not included in media level BFCP line in certain cases
CSCtq46039	cp-sip-trunk	Renegotiation SDP syntax incorrect for ANAT call
CSCtq47472	cp-sip-trunk	CUCM Codeyellow/Coredump due to SIP ICT connectivity lost.
CSCtq52484	cp-sip-trunk	4_parties_exit_conference_end_other-2-drop-call
CSCtq59044	cp-sip-station	softphone conference not working properly
CSCto58617	cp-sip-station	Servitude: Incoming call not working after 2 x blind transfers

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto66595	cp-sip-station	Cius re registers when an app is subscribed from CUCM
CSCtq00065	cp-sip-station	Speed dial w/ 9 prefix does not dial out
CSCtj87367	cp-sip-trunk	Code Yellow / Core Dump after upgrade
CSCtq57368	cp-sip-trunk	SIP Polycom doesnt negotiate video via h.323 trunkm
CSCtq67392	cp-sip-trunk	Transfer from CUCIMOC to E20 via h.323 trunk fails
CSCtn79239	cp-sip-trunk	CTS to VC call via a CUCM hop fails
CSCtq15868	cpi-appinstall	password from pwrecovery sometime no work after RU to new load
CSCtq52311	cpi-appinstall	install_log_migrate script failed to tar log files cause L2 upgrade fail
CSCtq66557	cpi-appinstall	L2 upgrade to 9.0 and above fails.
CSCtq68899	cpi-appinstall	Upgrade process needs to cleanup refresh upgrade files
CSCtq74591	ime-appinstall	IME Refresh upgrade on 7825H3 failed
CSCtq62914	ime-csa	After Switchback with IME to 8.51. from 8.6.1, wrong inactive version
CSCtq30093	cuc-tomcat	DT: Tomcat cores when using utils system restart
CSCtq38115	cpi-platform-api	getClusterNodes platform SOAP service only returns 1 node
CSCtq69347	cpi-os	IPv6 address not restore from backup
CSCtq71010	bps-bat	RU upgrade fails due to bps migration script failing
CSCtq71338	qed	Create New Product CSV file for AS Third Party SIP endpoint
CSCtq56857	dial-num-analyser	DNA not analyzing routes correctly - SQL error
CSCto43487	ccmcip	HEB: 8945: Hebrew personal directory service show up in English
CSCtg79013	security	tvs core when Pub/Sub1 switch back to old load after Sub2 install on new
CSCtq52222	selinux	Stopping auditd and setroubleshootd failures displayed during U1 boot up
CSCtq53442	cpi-os	7890C1 USB key present during re-image forces user interaction
CSCtq72631	security	TFTP Certificate in system file out of sync with database
CSCtq24472	cp-mediacontrol	No video after xfer : Allow2833 variable set incorrect
CSCtq73405	cp-mediacontrol	1-way video on SCCP Gumbo after TimeoutWaitingForVideoOLCAck

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq73524	cp-mediacontrol	1 way video with SCCP Gumbo to RT over DO SIP trunk
CSCtq74688	cp-mediacontrol	CTS 500 call gets dropped after the originator of the conference is rele
CSCtq76667	cmcti	CTIManager memory leak due to LDAP/SSL failures
CSCtq41065	cmcti	No ConnectedID with cbn number on DTAL after conference chain
CSCtq43478	cmcti	Incorrect partition is reported in CPIC after start whisper coaching
CSCtq73859	cp-supplementaryservices	Agent Greeting Call failure during load test
CSCto80476	jtapisdk	CallCtlConnDisconnectedEv received after TransferEnd
CSCtq55887	cp-mobility	CUCM phone and had RD pickup. Remote In Use is not there for Desktop
CSCtq71085	cp-mobility	Intelligent Session Control CFNA to VM uses cell as fwding DN
CSCtq18031	cp-mediacontrol	Failed media resource (MTP) allocation leads to CCM core
CSCto00448	cmui	Unable to access menus on CCM User page from native browser on CIUS
CSCto59013	cp-mediacontrol	No Video when CTS to EX90 call over H323 is hold/resume from CTS.
CSCtq13000	cp-sip-station	CM Coredump under traffic load.
CSCtq47636	cp-sccp	CUCM core on MB 8.6.1.10000-26
CSCtq43709	cpi-appinstall	L2 Upgrade Failure install_rpms
CSCto63870	cp-sip-station	503 Service unavailable in station_close state after SIP line reset
CSCtq42857	media_str_app	UCCX Intermittent Kernel Panic when Media --> Recording Step is Accessed
CSCtq41895	sa-maintenance	IE9: HTTP 404 status page on initiating Upgrade COP File in Morpheus
CSCtq35070	axl	AXLThrottler causing high Tomcat CPU
CSCtq22061	cp-mediacontrol	Can't resume SIPT call between Tandbergs with region pair at 32kbps
CSCto85294	cp-mobility	Mobility softkey / button stops working after failed hand-in
CSCto73185	vapi-real	RT Lite automation fails on makeCall
CSCto73005	cp-mgcp	CUCM responds with non user value to Status Enquiry
CSCto73285	webdialer-service	Webdialer - CTI service unavailable message not displayed

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCsr00340	cmui	Dependency records should show ExtensionMobilityDynamic records
CSCto74049	car	Summary report is calculating wrong data in Manager/Assistant report
CSCto80767	axl	Products assigned to users in CUCM are not showing up in CUPM
CSCto81448	cp-sip-trunk	Get no audio for mid-call transfer over SIP ANAT with MTP ICT
CSCto81820	cmui	Device profile disappears after saved in the app user CTI control Device
CSCto83868	cpi-os	7835/45-I3 fresh install has Raid firmware update failure
CSCto86462	cp-mobility	Mobility layer should send RelInd When DisconnReq contain Invalid CI
CSCto89349	cp-sip-station	Incorrect Fid used during Chaperone conference created with CallJoinReq
CSCto91102	bps-import-export	Validation for featurecontrolpolicy.csv failed in Export/Import Tool
CSCto91859	cp-sip-trunk	Hold on phone with SIPT--H.323 ICT hairpin transfer call will drop the c
CSCto94339	cp-sccp	Incorrect Fid used during Chaperone conference created with CallJoinReq
CSCto96231	axl	Can't assign the Moblity user ID using addPhone request
CSCtg41133	inter-dial-plan	Check-in of Text and Csv files for India,China into Clearcase
CSCto96586	cp-sip-trunk	No audio after blind transfer when SIP SP does not support UPDATE
CSCto98070	voice-sipstack	CUCM ignores subscribe refresh from TB endpoint
CSCto99256	cpi-os	CLI hangs with invalid login while enabling kdump for external SSHserver
CSCti60031	cp-sip-trunk	Re-order tone in originating side(CUCM) for unanswered CME call
CSCto99699	ccm-serviceability	Syntax error in naaagt script affects the naaagt's consistant performanc
CSCtj20695	rtmt	Alarm Definition Help not coming for Alarms with SubFacility having "_"
CSCtq06339	bps-import-export	Import of entities with no records showing error
CSCtj51295	cp-mediacontrol	CTS issue with CUCM reinvite with H.323 endpoints
CSCtj52266	tftp	MLPP domainId, MLPPIndication Status, Preemption from phone config page

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq07325	sa-mac	While configuring translation rules, rules vanishes randomly
CSCtq09875	axl	Get License Capabilities failed with UserID having Apostrophe
CSCtk11498	cmcti	Wrong Join/DT/JAL/DTAL info with default setting on 69xx/89xx-SIP
CSCtq11687	axl	UpdateUserGroup failed with UserID having Apostrophe
CSCtq11834	axl	UpdateLicenseCapabilities failed with UserID having Apostrophe
CSCtk65829	cp-mediacontrol	Call transferred to video device does not result in audio call overflow
CSCtq13534	cpi-os	"Error 15: File not found" shown in install log for install 8.6.1 on top
CSCtq13947	cpi-os	Update Python per RHSA-2011:0491-01 and RHSA-2011:0492-1
CSCtl43943	dial-num-analyser	DNA does not show local route group information
CSCtq15955	voice-sipstack	fix the SIP Stack SA warinng in MB 5-5-2011 report
CSCtq17311	media_str_app	Software MTP does not change payload type for RFC2833 DTMF
CSCtq18720	bps-bat	Bulk Administration file/log migration of RU from 7.1.5 to 8.6.1
CSCtl74266	cpi-afg	CUCM should validate X.500 O, OU string length in Answer File Generator
CSCtq20483	cp-sip-station	ATA 187fails for "Speed Dial Await Further Digits", if set to true
CSCtq24941	database	Fix SA warnings in cc_mainline for DBL2 MontBlanch issues
CSCtq27136	cp-sip-trunk	Refixing CSCti60031 - Re-order tone in originating side(CUCM) for unansw
CSCtq27720	cp-sip-station	connected number of the call back call is unknown
CSCtq28446	cp-bri	MontBlanc Static Analysis Issues related to MGCP Source files
CSCtq34932	cp-mgcp	DCP call hears ringback instead of MOH when MGCP is involved.
CSCtq35910	cpi-os	Cancel during install wizard detects existing good format as wrong one
CSCtn39639	cp-sip-station	CUCM incorrectly subscribes for KPML during CFW activation
CSCtq37461	cmui	CCMAdmin does not load properly on IE
CSCtq37975	cmcti	CTI manager using "NULL" devicePkid, causing CAD login issues

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtn51784	rtmt	Incorrect Error Message while launching RTMT
CSCtq38115	cpi-platform-api	getClusterNodes platform SOAP service only returns 1 node
CSCtq38433	cp-sip-trunk	S1/S2 Static Analysis error in sip-trunk and sip-line components
CSCtq40041	axl	Add Remote Destination Profile get failed with UserID having Apostrophe
CSCtq40768	tapisdk	LineGetCallInfo exception
CSCtq42131	sa-maintenance	Valid MD5 Checksum Validation Fails in Morpheus build
CSCtq43347	ccm-serviceability	L2 Upgrade Fails Due to CCM Service Not Registered in DB Correctly
CSCtq43523	cmui	Roaming Settings not shown in UI with high number of CSS or Device Pools
CSCtq43975	cp-sip-trunk	Calls in alpha failing due to issues with Early Media Cut-Through
CSCtn86627	bat	BAT:Assign 30K users to SC's failed, memory issue and Jabbard core
CSCtn87207	cp-mediacontrol	Two G729 calls consume 160kbp of location bandwidth
CSCtq44339	cp-sip-trunk	SIP layer sends out multiple codecs in the Offer when MTP required is ch
CSCtn97852	cpi-appinstall	"cimsubscribe" CORE due to RU server_specific_install.sh issue
CSCtq49089	axl	Remove Subscriber get failed with UserID having Apostrophe
CSCtq50205	cmui	ucmuser-beta contextlistener for locale
CSCtq51390	cp-pri	Incoming redirecting IE is discarded if digits are preficed with +
CSCtn99418	ccm-serviceability	CarIDSPerfmon Job Fail Alerts in Logged in Syslog File
CSCto01403	bps-import-export	Job status error during import in bulk admin tool
CSCtq54940	media_str_app	DTMF over RFC2833 fails as S/W MTP doesnt set correct seq number or SSRC
CSCtq55224	cmui	Phone configuration page takes long time to load
CSCtq57173	axl	Unable to perform Change Order for the attribute : Calling Search Space
CSCtq59447	bps-import-export	Import with override fails for CTIRoutePoint
CSCto07944	webdialer-service	Problem in interaction between Webdialer and EM service
CSCto11430	cp-rsvp-agent	Race condition leading to Contact Center Calls Get Stuck in Queue

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq63408	cp-mediacontrol	Renegotiation during MeetMe with MTP has wrong profile level.
CSCtq65343	vapi-real	complete and commit changes to merlin for gumbo sccp support
CSCtq69347	cpi-os	IPv6 address not restore from backup
CSCto25077	cp-sip-station	Sip phone hears ringback tone when calling busy line on PRI
CSCtq79105	voice-sipstack	Fix handling of dbl incremented cseq
CSCto36517	bps-import-export	Users Associated with Line is not exported by BAT
CSCto43412	cp-supplementaryservices	Hunt Call hang when conferneced call go back to 2 party call
CSCto45744	cp-mediacontrol	EX90 to EX90 E2E RSVP call failing when region pair max audio is 32 kbps
CSCto45772	cp-mediacontrol	H323-SIPICT-E20 hold/resume from E20 doesn't work for Audio G7221 codec
CSCto45800	cp-mobility	MGCP EFA call got busy tone with Dragon login
CSCto46211	tapisdk	no CONFERENCED call state on Target in app on cBarge
CSCto50580	cp-sip-trunk	One way video on RT with call flow RT-VCS/C20--need updated Lua script
CSCto50730	cp-mobility	Dragon DVO transfer/add call doesnt work
CSCto51150	database	setrepltimeout command does not indicate success/failure of command
CSCto52071	cpi-os	dhcpd req's manual restart if NFT enabled/disabled
CSCto53232	voice-sipstack	CUCM ignores subscribe refresh from TB endpoint
CSCto54048	cmcti	CTI Manager not reporting the correct device handle
CSCto56209	cp-sip-trunk	CUCM includes diversion header when doing called party transformation
CSCto58469	cp-sip-trunk	Secure/encrypted call to SIP Service Provider call disconnects after OK
CSCto58904	cp-mediacontrol	Floor control role incorrect in re-INVITE glare scenario
CSCto60019	cli	utils network ipv6 traceroute command does not work
CSCto60097	tapisdk	Dynamic tracing is not working if app opened Provider and lines
CSCto60189	cp-mobility	Android can't reg as VOIP when MI not config'd after trying reg as cell
CSCto62746	voice-sipstack	FECC does not function on MXP 1500 (H.323)
CSCto66019	cp-mobility	correct Cisco Dual Mode for Android product and model monikers

Table 3 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto70180	cp-mediacontrol	Call between RT & TB drops on resuming the call on RT phone.
CSCto70998	cp-mediacontrol	Inter-cluster video call between LS & TB establishes as audio call.
CSCto71473	cp-mediacontrol	meetMee_wrong_reservation-410
CSCto72113	cpi-appinstall	Upgrade process tries to switch version even though upgrade does not com
CSCto72188	jtapisdk	Get NPE on conference with codian conference bridge

Documentation Updates

The Documentation Updates section contains information about errors, omissions, and changes for the Cisco Unified Communications Manager documentation and online help.

Online Help for Called Party Tracing Window Is Missing

The online help for the Called Party Tracing window is missing in Cisco Unified Communications Manager Administration. The error can be located by clicking Advanced Features > Called Party Tracing; then, by clicking Help > This Page.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop by using a reader application. Be aware that the RSS feeds are a free service, and Cisco currently supports RSS version 2.0.