Release Notes for Cisco Unified Communications Manager Release 8.6(2)

August 29, 2013

Note You can view release notes for Cisco Unified Communications Manager Business Edition 5000 at http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html.

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/sw/voicesw/ps556/prod_release_notes_list.html.

Table 1 Updates to Release Notes for Cisco Unified Communications Manager 8.6(2)

Date	Changes
09-25-13	Added a note about externally-powered USB to the Upgrade section.
08-09-13	Added CSCug38337 TFTP Service Parameter "Maximum Serving Count", page 65 to Documentation Updates
07-05-13	Added CSCuh62299 Note added to the Service Name field, page 69 to Documentation Updates
21-01-13	Added CSCue04792 EMCC Logout Limitation, page 28 to Important Notes, page 27.
04-01-13	Added CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 46 to Important Notes, page 27.
13-01-02	Added CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT, page 29 to Important Notes, page 27.
12-11-12	Added CSCud57169 CTL file size limit of 32 kilobytes should be 64 kilobytes, page 46 to Important Notes, page 27.
12-5-12	Added CSCud34740 Application User AXL Password Must Not Contain Special Characters, page 45 to Important Notes, page 27.
10-31-12	Added CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none> and CSCtw44980 Missing Exceptions for Voice-Mail Pilot to Important Notes.

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

Table 1 Updates to Release Notes for Cisco Unified Communications Manager 8.6(2)

Date	Changes
10-3-12	Added CSCuc39511 Expansion module field missing from certain device profiles, page 29 to Important Notes.
10-3-12	Added CSCtb31860 Transcoding G.711 to All Codecs Supported, page 29 to Important Notes.
09-28-12	Added CSCuc30279 Cannot Disassociate Devices From End Users Using BAT, page 29 to Important Notes.
09-21-12	Added CSCuc10415 Tip for Adding a New Server, page 45 to Important Notes.
09-18-12	Updated Documentation Updates, page 64: added Device Name and Description fields need to be updated, page 64.
09-10-12	Added a note about IP phone firmware to the "Post-Upgrade Tasks" section on page 20.
08-31-12	Updated the "Important Notes" section on page 27 (added CSCtc71174 Call Park and Directed Call Park Restriction, page 44).
08-24-12	Updated the "Important Notes" section on page 27. Added the following: • CSCtr78911 Answer Too Late Timer, page 29 • CSCts83374 Remote Destination Configuration Settings for Single Number Reach and Reroute Remote Destination Calls to Enterprise Number, page 30 • CSCto57498 Upgrading to Cisco Unified Communications Manager Release 8.x from Release 7.x, page 30
08-09-12	Updated the "Important Notes" section on page 27 (added CSCtd69640 Downtime when upgrading Publisher server until all Subscriber servers are updated, page 31).
08-02-12	Updated Important Notes, page 27 and added CSCtk68384 Disable ICH10 onboard SATA controller on EX/ESXi servers during Unified CM installation, page 32.Updated the following sections for
07-30-12	Updated Important Notes, page 27 and added CSCub10861 Call waiting behavior with MLPP Preemption correction, page 32.Updated the following sections for
07-25-12	Updated the "Important Notes" section on page 27 . Added the following: • CSCua01779 Cisco Unified Communications Manager Locale Installer locale file for Belgium, page 32) • CSCtz88812 Cisco IP Phones and Cisco Unity Connection support for IPv6, page 32 Updated the Documentation Updates, page 64 and added Cisco Unified Communications Manager TCP and UDP Port Usage Guide, page 70.
7/18/12	Updated Important Notes, page 27 and added CSCte39796 Increase database replication timeout when upgrading large clusters, page 33.Updated the following sections for
7/12/12	Updated Important Notes, page 27 and added CSCsy57492 Hold Reversion Notification Interval for SCCP and SIP phones, page 33.
6/26/12	Updated Important Notes, page 27 and added New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651), page 33.

Table 1 Updates to Release Notes for Cisco Unified Communications Manager 8.6(2)

Date	Changes
9/29/11	Updated the following sections for Cisco Unified Communications Manager information for Release 8.6(2): • Caveats, page 56
9/23/11	Updated the following sections for Cisco Unified Communications Manager information for Release 8.6(2): • Important Notes, page 27
09/15/11	Updated the following sections for Cisco Unified Communications Manager information for Release 8.6(2): • Introduction, page 4 • System Requirements, page 4 • Upgrading to Unified CM 8.6(2), page 6 • Related Documentation, page 26 • Limitations and Restrictions, page 26 • Important Notes, page 27 • Caveats, page 56 • Documentation Updates, page 64

Contents

This document includes the following information:

Before you install or upgrade Cisco Unified Communications Manager (Unified CM), Cisco recommends that you review the "Upgrading to Unified CM 8.6(2)" section on page 6, and the "Latest Software and Firmware Upgrades for Unified CM 8.6 on Cisco.com" section on page 26 for information pertinent to installing or upgrading, and the "Important Notes" section on page 27 for information about issues that may affect your system.

Note The Cisco Unified Communications Manager 8.6(2) documentation collection consists of the following: New and Changed Information, Release Notes, the Documentation Guide and the Compatibility Matrix. You must use these documents in conjunction with the complete documentation collection for Unified CM 8.6(1).

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.

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.

For supported Virtualization of Cisco Unified Communications Manager, see www.cisco.com/go/uc-virtualized.

Note Make sure that the matrix shows that your server model supports Unified CM Release 8.6(2).

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(2). 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.

Note When the MCS-781x and MCS-782x servers are not connected to a UPS, they run a higher risk of file corruption during power outages, as the cached data is lost during a power outage on these servers with drive write cache enabled (and no battery backup). To prevent file system corruption, you must connect these servers to a UPS.

When Unified CM runs on one of the servers listed in Table 2, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB is supported.

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.

Table 2 Supported Servers for UPS Integration

HP Servers	IBM Servers	UCS Servers
MCS-7816-H3	MCS-7816-I3	B200 M1 Blade Server[1]
MCS-7825-H3	MCS-7816-I4	B200 M2 Blade Server
MCS-7825-H4	MCS-7816-I5	C200 M2 Rack Server
MCS-7828-H3	MCS-7825-I3	C210 M1 Rack Server
MCS-7835-H2	MCS-7825-I4	C210 M2 Rack Server
MCS-7845-H2	MCS-7825-I5	
	MCS-7828-I3	
	MCS-7828-I4	
	MCS-7828-I5	
	MCS-7835-I2	
	MCS-7845-I2	
	MCS-7835-I3	
	MCS-7845-I3	

1. For information on End of Sale and End of Life status on Cisco Unified Computing System servers, consult http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_eol_notices_list.html for Collaboration part numbers and http://www.cisco.com/en/US/products/ps10493/prod_eol_notices_list.html for Data Center part numbers.

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(2)

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

Caution When you upgrade to Cisco Unified Communications Manager 8.6(2), 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(2), 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(2) 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.

Note 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.

Software Version Number

These release notes are based on following software version:

- Unified CM: 8.6.2.10000-30

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

- 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.
- 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 9.

Software Upgrade Considerations

This section contains the following topics:

Overview of the Software Upgrade Process

With this version of Cisco Unified Communications Manager, 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 a 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.

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.

When you upgrade a cluster, you start by upgrading the first node. Once the upgrade on the first node completes, you can begin upgrading subsequent nodes in parallel.

All servers in a cluster must run the same release of Cisco Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

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.

If the upgrade of a subsequent node fails after you upgrade the first node and switch it to the new version or fail to upgrade one of the subsequent nodes in your cluster during the upgrade cycle, you can do one of the following:

- Correct the errors that caused the upgrade failure on the subsequent node. You may want to check the network connectivity of the nodes in your cluster, reboot the subsequent node, ensure the server memory and CPU usage on the subsequent node are not too high. Upgrade the subsequent node again.
- Make sure that the active partition of the first node runs the newest version of software installed on the server. Perform a fresh installation on the subsequent node using the same software version as that running on the active partition of the first node. If you are reinstalling the subsequent node, you should delete the server from Cisco Unified Communications Manager Administration and add the server again as described in the *Cisco Unified Communications Manager Administration Guide*.

You can upgrade from a DVD (local source) or from a network location (remote source) that the Cisco Unified Communications Manager 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(2) on a Virtual Server

If you run Cisco Unified Communications Manager on a virtual server, and are upgrading to the 8.6(2) 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).

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

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. 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

Supported Upgrades

For information about supported upgrades, the Cisco Unified Communications Manager Compatibility Matrix at the following URL:

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

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(2) 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:

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_v1.0.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(2)

If upgrading from 8.5(1) or earlier complete the "Installing the COP File" section on page 14.

Note The unrestricted version of Unified CM 8.6(2) 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_8.6.2.10000-30.sgn.iso

For the unrestricted version:
UCSInstall_UCOS_UNRST_8.6.2.10000-30.sgn.iso

Note Because the UCSInstall_UCOS_8.6.2.10000-30 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:

65ba754dd1078abed951fe705d0854e3 UCSInstall_UCOS_8.6.2.10000-30.sgn.iso

For the unrestricted version:

b87b58295237adb24341a090d2836285 UCSInstall_UCOS_UNRST_8.6.2.10000-30.sgn.iso

Step 3 Continue by following the instructions in Upgrading from a Local Source, page 15 or Upgrading from a Remote Source, page 16.

Upgrading 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 14.

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 do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Note Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks.

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 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 14 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 15 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 16 When the installation completes, click **Finish** (not applicable for Refresh Upgrades).

Step 17 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).

Upgrading from a Remote Source

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.

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 14.

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 Log in to Cisco Unified Communications Operating System Administration.

Step 5 Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

Step 6 From the **Source** list, choose **Remote Filesystem**.

Step 7 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 8 In the **Server** field, enter the server name or IP address.

Step 9 In the **User Name** field, enter your user name on the remote server.

Step 10 In the **User Password** field, enter your password on the remote server.

Step 11 Select the transfer protocol from the **Transfer Protocol** field.

Step 12 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 13 To continue the upgrade process, click **Next**.

Step 14 Choose the upgrade version that you want to install and click **Next**.

Step 15 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 16 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 17 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 18 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 19 When the installation completes, click **Finish** (not applicable for Refresh Upgrades).

Step 20 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.

Note After you perform a switch version when you upgrade Unified CM, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

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.

This section contains the following topics:

- Reverting the Publisher or Subscriber Nodes to a Previous Version, page 22
- Resetting Database Replication When Reverting to an Older Product Release, page 22

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.

Reverting a Cluster to a Previous Version

Note If you downgrade a cluster to a nonsecure previous release of Cisco Unified Communications Manager (releases prior to Release 8.0), you must prepare the cluster for rollback before you switch versions. If you do not prepare the cluster for rollback before you revert to a previous release, you will have to manually delete the ITL file on each Cisco Unified IP Phone in the system. For more information, see Chapter 2, "Security by Default," in the *Cisco Unified Communications Manager Security Guide*.

To revert a cluster to a previous version, follow these major steps:

	Task	For Additional Information
Step 1	Revert the publisher node.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 22.
Step 2	Revert all backup subscriber nodes.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 22

	Task	For Additional Information
Step 3	Revert all primary subscriber nodes.	"Reverting the Publisher or Subscriber Nodes to a Previous Version" section on page 22
Step 4	If you are reverting to an older product release, reset database replication within the cluster.	"Resetting Database Replication When Reverting to an Older Product Release" section on page 22

Reverting the Publisher or Subscriber Nodes to a Previous Version

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 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.

Resetting Database Replication When Reverting to an Older Product Release

If you revert the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command **utils dbreplication reset all** on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message that reminds you about the requirement to reset database replication if you are reverting to an older product release.

Installing COP Files, Dial Plans, and Locales

This section contains the following topics:

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 "Upgrading from a Local Source" section on page 15 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.

Note The Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

Changes do not take effect until you reboot every server in the cluster. Cisco strongly recommends that you do not reboot the servers until you have installed all locales on all servers in the cluster. Minimize call-processing interruptions by rebooting the servers after regular business hours.

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 "Upgrading from a Local Source" section on page 15 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 24 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

Error Messages

See Table 1-3 for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 1-3 Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.

Table 1-3 Locale Installer Error Messages and Descriptions (continued)

Message	Description
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable	This error occurs because a Cisco Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Cisco Unified Communications Manager database. If this application is not found, it either was not installed with Cisco Unified Communications Manager (very unlikely), has been deleted (more likely), or the server does not have Cisco Unified Communications Manager installed (most likely). Installation of the locale will terminate because locales will not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, /usr/local/thirdparty/java/j2sdk/jre/bin/java, an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Supported Cisco Unified Communications Products

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the *Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager*, which is available at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51

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(2) at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_6_2/rel_notes/ime-rel_notes-862.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(2) 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(2). 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(2).

CSCue04792 EMCC Logout Limitation

In the visiting cluster, the current Phone Configuration window has a Log Out button for intracluster EM. This button is also used by the visiting cluster administrator to logout an EMCC phone. Because the EMCC phone is not currently registered with the visiting Cisco Unified Communications Manager, this operation is equivalent to a DB cleanup in the visiting cluster. The EMCC phone will remain registered with the home Cisco Unified Communications Manager until it comes back to the visiting cluster due to a reset or a logout from the home cluster by other means.

CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT

Cisco Unified Communications Manager VMware installations can experience high CPU usage spikes while performing tasks such as DRF backups and Bulk Administration Tool exports. The processes that are commonly responsible for CPU usage spikes are gzip and DRFLocal.

If your system is generating CallProcessingNodeCpuPegging alarms, add an additional vCPU for the support of 7500 Cisco Unified Communications Manager users following the Open Virtualization Archives (OVA) template specifications.

During CPU usage spikes, other alarms that may be issued in addition to the CallProcessingNodeCpuPegging alert include: CoreDumpFound, CriticalServiceDown, SDLLinkOutOfService, and NumberOfRegisteredPhonesDropped alarms.

CSCuc39511 Expansion module field missing from certain device profiles

The expansion module field is not listed on the Device Profile Configuration window for Cisco Unified IP Phone models 8961, 9951, and 9971. No manual selection is required. The lines from the Phone Button Template are applied to the physical device no matter which expansion modules these phones use.

Skip step 9 in the procedure to "Create the device profile for a user"as documented for Cisco Extension Mobility configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 9 If the phone type supports Cisco Unified IP Phone Expansion Modules, Cisco Unified Communications Manager displays expansion module field. At the Module 1 drop-down list box and at the Module 2 drop-down list box, choose the appropriate expansion module.

CSCtb31860 Transcoding G.711 to All Codecs Supported

The transcoder supports transcoding between G.711 and all codecs, including G.711, when functioning as a transcoder and when providing MTP/TRP functionality.

CSCuc30279 Cannot Disassociate Devices From End Users Using BAT

The Bulk Administration Tool (BAT) cannot be used to disassociate devices that are already associated to an end user.

If you manually delete a controlled device from an exported end-user record and then insert the modified user record back in to the Cisco Unified Communications Manager database as a custom CSV data file, the insertion appears successful when you check the job results using **Bulk Administration > Job Scheduler**. However, the controlled device is still listed on the End User Configuration window in Cisco Unified Communications Manager Administration.

CSCtr78911 Answer Too Late Timer

In Cisco Unified Communications Manager Administration, use the **Device > Remote Destination** menu path to configure remote destinations.

Answer Too Late Timer

Enter the maximum time in milliseconds that Cisco Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Cisco Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise.

Range: 0 and 10,000 - 300,000 milliseconds

Default: 19,000 milliseconds

If the value is set to zero, the timer is not started.

CSCts83374 Remote Destination Configuration Settings for Single Number Reach and Reroute Remote Destination Calls to Enterprise Number

In Cisco Unified Communications Manager Administration, use the **Device > Remote Destination** menu path to configure remote destinations.

Single Number Reach

You can configure all of the Remote Destination Configuration Settings for Single Number Reach.

Reroute Remote Destination Calls to Enterprise Number

For the Reroute Remote Destination Calls to Enterprise Number, you can configure:

- Answer Too Soon Timer
- Answer Too Late Timer

For the Reroute Remote Destination Calls to Enterprise Number, you can *not* configure:

- Delay Before Ringing Timer
- Enable Mobile Connect
- Ring Schedule

CSCto57498 Upgrading to Cisco Unified Communications Manager Release 8.x from Release 7.x

To upgrade your cluster from Release 7.x to Release 8.x, follow this procedure:

Procedure

Step 1 Follow the normal procedure for upgrading a cluster.

Tip After you finish upgrading all nodes in the cluster to Cisco Unified Communications Manager Release 8.x, you must also follow all the steps in this procedure to ensure that your Cisco Unified IP Phones register with the system.

Step 2 If you are running one of the following releases in mixed mode, you must run the CTL client:

Cisco Unified Communications Manager Release 7.1(2)

- All regular releases of 7.1(2)

- All ES releases of 712 prior to 007.001(002.32016.001)

Cisco Unified Communications Manager Release 7.1(3)

- All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
- All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see Chapter 4, "Configuring the CTL Client," in the *Cisco Unified Communications Manager Security Guide*.

Restart the Cisco TFTP Service on the TFTP Servers

Step 3 From Cisco Unified Serviceability, choose **Tools > Control Center - Feature Services.**

The Control Center - Feature Services window displays.

Step 4 Restart the Cisco TFTP service on each node on which it is active.

Step 5 Wait five minutes for TFTP to rebuild the files.

Reset all Cisco Unified IP Phones

Note You must reset all the Cisco Unified IP Phones in the cluster to ensure that the phones have the most current configuration.

Step 6 From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

The Enterprise Parameters Configuration window displays.

Step 7 Click **Reset**.

Step 8 Wait ten minutes for the Cisco Unified IP Phones to register with Cisco Unified Communications Manager.

Back Up Your Cluster

Caution You must back up your cluster using the Disaster Recovery System (DRS) to be able to recover the cluster.

Step 9 To backup your cluster using DRS, see the *Disaster Recovery System Administration Guide*.

CSCtd69640 Downtime when upgrading Publisher server until all Subscriber servers are updated

When upgrading the publisher node, there will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

CSCtk68384 Disable ICH10 onboard SATA controller on EX/ESXi servers during Unified CM installation

If the server is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi. Perform the following steps to disable the SATA controller in the BIOS as a pre-installation task when installing the Cisco Unified Communications Manager.

1. Boot the server and press F2 when prompted during bootup.
2. Select Advanced tab.
3. Select Mass Storage Controllers Configuration.
4. Set the Onboard SATA Controller to Disabled.

CSCub10861 Call waiting behavior with MLPP Preemption correction

When a Routine precedence call is offered to a destination station that already has active calls that are configured with call waiting, normal call waiting is activated if the existing call count is less than the busy trigger.

When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, precedence call waiting is activated if the existing call count is less than the busy trigger and any of the following conditions exist:

- The device supports visual call appearances and has an open appearance.
- The device supports two non-visual call appearances and has an open appearance, and the precedence of the new call is equal to or lower than the existing call.
- The device has an open appearance (visual or non-visual) and the device is non-preemptable.

When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, an existing lower-precedence call is preempted if the existing call count is equal to or greater than the busy trigger.

CSCua01779 Cisco Unified Communications Manager Locale Installer locale file for Belgium

Since the primary language spoken in Belgium is Dutch, you can download the Dutch (Netherlands) locale file, for example, cm-locale-nl_NL- 8.5.1.2100-1.cop.sgn (Cisco Unified Communications Locale Installer 8.5.1.21000-1 Dutch (Netherlands)). Secondary languages commonly spoken in Belgium are French and German.

CSCtz88812 Cisco IP Phones and Cisco Unity Connection support for IPv6

For information about IPv6 support for your IP phone or Unity Connection, see the Cisco Unified IP Phone Administration Guide that supports your phone model or the Cisco Unity Connection documentation.

CSCte39796 Increase database replication timeout when upgrading large clusters

Use the **utils dbreplication setrepltimeout** CLI command to increase the database replication timeout value when upgrading large clusters so that more subscriber servers have sufficient time to request replication. When the timer expires, the first subscriber server, plus all other subscriber servers that requested replication within that time period, begin a batch data replication with the publisher server. The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the subscriber servers have successfully set up replication. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

CSCsy57492 Hold Reversion Notification Interval for SCCP and SIP phones

SCCP phones support a minimum Hold Reversion Notification Interval (HRNI) of 5 seconds, whereas SIP phones support a minimum of 10 seconds. SCCP phones set for the minimum HRNI of 5 seconds may experience a Hold Reversion Notification ring delay of 10 seconds when handling calls involving SIP phones.

New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651)

A new license file is required if you are installing a replacement motherboard in publisher servers or single servers that are not part of a cluster.

Internet Protocol Multimedia Subsystem IMS Service Control Interface Support

The Internet Protocol Multimedia Subsystem IMS Service Control Interface is not supported in Cisco Unified Communications Manager 8.6(2).

H.323 Client Device Name

You must give an H.323 client a device name between 1 and 50 characters. The name may consist of upper and lower case letters; numbers (0-9); periods (.); underscores (_); or dashes (-).

Please avoid any other special characters in an H.323 device name, otherwise the error message "unmapped Exception null" is displayed.

Disaster Recovery System Enhancements

Estimating The Size of The Backup Tar

Follow this procedure to estimate the size of the backup tar performed on an SFTP device.

Note Be aware that the calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup. Also, this procedure does not estimate the size of a backup performed on a tape device.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration, choose Cisco Unified Communications Manager from the Navigation menu in the upper right corner and click **Go**. The Disaster Recovery System Sign-In window appears.

Step 2 Sign in to the Disaster Recovery System by using the same administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup > Manual Backup**. The Manual Backup window appears.

Step 4 In the Select Features area, select the features to back up.

Step 5 To get the estimated size of backup for the selected features, click **Estimate Size**.

Caution Be aware that if no backup history exists for one or more of the selected features, Cisco Unified Communications Manager cannot estimate the size of the backup tar.

Starting A Manual Backup

Caution Be aware that error messages such as “no space in remote server” or “network transfer rate is very slow” may appear. If the backup tar size does not increase for 15 minutes, the backup process fails. Address the problem that caused the backup to fail and then start a fresh backup.

Command Line Interface

Table 4 Disaster Recovery System Command Line Interface

Command	Description
utils disaster_recovery estimate_tar_size	Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list

Auto Update Statistics (AUS)

In earlier releases of Cisco Unified Communications Manager, the Cisco Database Layer Monitor service parameters **Maintenance Throttling for Tables** and **Maintenance Throttling for Stored Procedures** controlled the process for updating statistics about indexes. Now, Cisco Unified Communications Manager 8.6(2) uses Automatic Update Statistics, an intelligent statistics update

feature that monitors the changes made in the database tables and updates only tables that need statistic updates. This feature saves considerable bandwidth, especially on VMware deployments of Unified CM. Automatic Update Statistics is now the default indexing method.

Cluster-Wide Call Park

Cisco Unified Communications Manager 8.6(2) allows you to enable call parking for cluster-wide configurations. The following changes are introduced with this feature:

- Park codes for all nodes in a Cisco Unified Communications Manager cluster are now allocated from a single entity, the lowest active node in the cluster. Therefore, Unified CM ignores the Cisco Unified Communications Manager field on the Call Park Configuration web page.
- The single entity allocates park codes from a pool of all configured park codes, regardless of which Unified CM is assigned.
- Unified CM allocates park codes through strict enforcement of the partition order in the Calling Search Space (CSS) of the parking party. This update provides a predictable behavior that is easy for administrators to understand.
- The parked calls limit is no longer 100 calls per cluster. Available park codes and system resources determine the number of parked calls.
- CTI monitoring of parked call Directory Numbers (DNs) is unavailable. This function will be restored in Unified CM Release 9.0.

CallPark Softkey

After the called party presses the CallPark softkey to park a call, Unified CM 8.6(2) takes the following actions to allocate a park code:

- The unique Unified CM node with the active CallParkCodeManager process allocates a park code.
- Unified CM checks the partition list of the CSS of the parking party for available park codes by searching each partition in order. If Unified CM finds a code, the system allocates the code and marks it as unavailable. If Unified CM does not find an available code in any of the partitions, the call park attempt fails.

Previous Call Park Behavior

In previous releases of Unified CM, the following actions occurred:

- The Unified CM node where the call originates (any node in the cluster) allocated a park code from the pool of codes that were assigned to that Unified CM node.
- Unified CM checked the list of available park codes, regardless of their partition order, to detect whether these codes existed in the CSS of the parking party. If Unified CM found an available code, the system allocated the code and marked it as unavailable. If Unified CM found no available code on the partitions, the call park attempt failed.

New Call Park Behavior

With these new Call Park behaviors, centralized Unified CM deployments that host multiple locations on a single cluster (such as retail stores and bank branches) can now place the park codes for each location into the partitions that are devoted to those locations. This placement prevents parties at one store from retrieving calls parked at another store. Also, the new Call Park behaviors reduce the difficulty of administering the feature, because administrators no longer need to place park codes in the CSS of each inbound trunk.

Finally, this behavior follows the partition order of a CSS when searching for objects, which aligns with the search behaviors of other Unified CM features described in the SRND. This behavior makes Call Park easier to understand, because administrators no longer need to assign park codes to every Unified CM node on the side where a call originates.

Enabling Cluster-Wide Call Park

To enable Cluster-Wide Call Park, perform the following steps:

Step 1 From Cisco Unified Communications Manager Administration, select **Advanced Service Parameters > Global Features**

Step 2 Set the Enable Clusterwide CallPark Number/Ranges service parameter to True.

Step 3 Restart all Unified CM services.

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

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

```
utils diagnose module raid
```

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, DNS configuration, version and the deployment type must be the same as it was during the backup. DRS does not restore across different hostnames, IP addresses, DNS configurations, 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.

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 release 8.6.(x) is interoperable with a Cisco TelePresence Video Communication Server (VCS) X6.1 and above using a Session Initiation Protocol (SIP) Trunk. 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.

In release 8.5(x) of Cisco Unified Communications Manager, the script had to be manually created/imported into Cisco Unified Communications Manager, but Release 8.6(1) and above includes the script and does not need to be manually created/imported. The name of the script included in release 8.6(1) and above is *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(2).

- VCS Interoperability SIP Normalization Script Issues for Upgrades to Release 8.6(2), page 38
- Configuring VCS Interoperability SIP Normalization Script in Release 8.6(2), page 39

VCS Interoperability SIP Normalization Script Issues for Upgrades to Release 8.6(2)

If you are upgrading to Cisco Unified Communications Manager 8.6.2 from a 8.5(x) release, and you had previously created/imported a SIP Normalization Script for VCS interoperability, the upgrade to 8.6(2) will fail if the name of the SIP Normalization Script used in your previous release is *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(2):

Note Renaming the existing script is not required for upgrades from release 8.6(1) to 8.6(2). It is only required for upgrades from a 8.5(x)release to release 8.6(1) and above.

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 included in the 8.6 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*. For example, you may want to rename it to *vcs-interop-old* or *vcs-interop-8.5*.

b. Click Reset.

Step 4 Proceed with the upgrade.

After upgrading to 8.6(2), complete Configuring VCS Interoperability SIP Normalization Script in Release 8.6(2), page 39 to configure VCS interoperability SIP Normalization Script in Release 8.6(2).

Configuring VCS Interoperability SIP Normalization Script in Release 8.6(2)

After installing or upgrading to Cisco Unified Communications Manager 8.6(2), perform the following steps to configure Cisco Unified Communications Manager to use the new *vcs-interop* script for all existing SIP trunks to/from 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**.

Configuring a SIP Trunk between CUCM and VCS

The following describes how to configure a SIP Trunk between Cisco Unified Communications Manager and VCS. The SIP Trunk configuration spans the following pages in Cisco Unified Communications Manager Administration:

- SIP Trunk Security Profile
- SIP Profile
- SIP Trunk
- Enterprise Parameters
- Service Parameters

SIP Trunk Security Profile (System > Security > SIP Trunk Security Profile)

The following fields in the SIP Trunk Security Profile Configuration page should be configured as shown in Table 5. For more information on the definition and use of each field, refer to the online help in Cisco Unified Communications Manager Administration (**Help > This Page**).

Table 5 SIP Trunk Security Profile configuration for VCS

Field	Setting	Comment
Name	Any Name	e.g. VCS SIP Trunk Security Profile
Description	Any Description	e.g.Secure TLS for VCS Trunk
Device Security Mode	Encrypted	Encrypted is recommended. Non Secure and Authenticated are also supported.

Field	Setting	Comment
Incoming Transport Type *	TLS	TLS is recommended. TCP+UDP is also supported when Non Secure mode is selected.
Outgoing Transport Type	TLS	TLS is recommended. TCP and UDP are also supported when Non Secure mode is selected.
Enable Digest Authentication	Unchecked	Digest Authentication is optional
X.509 Subject Name	TANDBERG	The common name of the default VCS certificate is TANDBERG (e.g. CN=TANDBERG). If VCS is using a different certificate, use the Common Name of that certificate in the X.509 Subject Name field instead of TANDBERG.
Incoming Port*	5061	5061 is recommended when Encrypted Mode is selected. 5060 is recommended when Non Secure mode is selected.
Enable Application Level Authorization	Unchecked	Application Level Authorization is only needed if there are multiple devices on VCS sending requests to CUCM and you want to enable/disable features per device/user.If you check this checkbox, you must also check the Enable Digest Authentication check box and configure digest authentication for the trunk.
Accept Presence Subscription	Checked	Presence Subscription is optional.
Accept Out-of-Dialog REFER**	Checked	Out-of-Dialog REFER is optional.
Accept Unsolicited Notification	Checked	Unsolicited Notification is optional.
Accept Replaces Header	Checked	Replaces Header support is optional.
Transmit Security Status	Checked	Transmits the security icon status of calls to/from the VCS.

SIP Profile configuration (Device > Device Settings > SIP Profile)

The following fields in the SIP Profile Configuration page should be configured as shown in Table 6. Only the fields that must be configured with a specific value are shown. All other fields may be left at their default values. For more information on the definition and use of each field, refer to the online help in Cisco Unified Communications Manager Administration (**Help > This Page**).

Table 6 SIP profile configuration

Field	Setting	Comment
Redirect by Application	Enable	Required for processing Call Forwarding and Multiway MCU redirection requests received from VCS
Use Fully Qualified Domain Name SIP Requests	Enable	For this parameter to take effect, the Enterprise Parameter (System > Enterprise Parameters) Organization Top Level Domain parameter must als be set.
Allow Presentation Sharing using BFCP	Enable	
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	Enable	

SIP Trunk configuration (Device > Trunk > SIP Information)

The following fields in the SIP Trunk Configuration page must be configured as shown in Table 7. Only the fields that must be configured with a specific value are shown. All other fields may be left at their default values. For more information on the definition and use of each field, refer to the online help in Cisco Unified Communications Manager Administration (**Help > This Page**).

Table 7 SIP trunk configuration

Field	Setting	Comment
SRTP Allowed	Enabled	
Redirecting Diversion Header Delivery - Inbound	Enabled	Required if VCS is directly integrated with Cisco Unity voicemail
Redirecting Diversion Header Delivery - Outbound	Enabled	Required if VCS accesses Cisco Unity voicemail indirectly through CUCM
Destination Address [1-6]	IPv4 address or hostname of VCS	Add one entry for each VCS node within the VCS cluster to which CUCM is neighboring to
Destination Port [1-6]	5061 if SIP Trunk Security Profile is configured for Authenticated or Encrypted modes, 5060 if SIP Trunk Security Profile is configured for Non Secure mode	Must match the port VCS is configured to listen on in VCS Administration for the Neighbor Zone between VCS and CUCM (VCS Configuration > Zones)
SIP Trunk Security Profile	Security Profile configured for VCS trunk	
Rerouting Calling Search Space	configure to suit your environment	The Rerouting Calling Search Space is used for processing Transfer and Multiway MCU redirection requests received from VCS
SIP Profile	SIP Profile configured for VCS trunk.	
Normalization Script	"vcs-interop"	Leave the Enable Trace disabled and the Parameter Name and Parameter fields blank unless instructed otherwise by Cisco Technical Assistance (TAC)

Enterprise Parameters (System > Enterprise Parameters)

The Organization Top Level Domain parameter should be set according to your organization domain name (e.g. company.com). This parameter is then used by the **SIP Profile > Use Fully Qualified Domain Name** in SIP Requests parameter when processing calls to and from VCS.

Service Parameters (System > Service Parameters > Cisco CallManager > Advanced)

The SIP Max Incoming Message Size parameter should be set to 11000 bytes to ensure successful negotiation of secure RTP (sRTP) between CUCM and VCS devices. In release 8.6(2) the default value of this parameter was increased from 5000 to 11000. Verify that the parameter is set to 11000.

For more information, see the Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide (CUCM 6.1,7,8 and X7) which is available at

http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Cisco_Unified_Communications_Manager_Deployment_Guide_CUCM_6-1_7_8_and_X7-0.pdf

CSCts13972 Must re-run CTL Client when the Domain Name Changes

When a domain name is added or changed on a Cisco Unified Communications Manager cluster in mixed mode, you must re-run the CTL Client or changes to the phone configuration files do not take effect.

CSCts35326 "KERNEL: assertion (!sk->sk_forward_alloc) failed at net/ipv4/af_inet.c (152)" Displayed on Console Screen

This may display on the console screen when running IMS calls due to an issue with RedHat (case 00522987). It does not cause any IMS call failures. These messages can be ignored if they are not causing any issue on the system.

Deploying the SAF Call Control Discovery Feature

If you are considering deploying the SAF Call Control Discovery feature, do not clone publishers and use the new identity feature to build out multiple clusters. The new identity feature does not currently support regenerating a unique id for the cluster, and SAF Call Control Discovery will not function properly without unique cluster identification.

CSCtr54150 Mobile Voice Access over SIP trunks and H.323 Gateways

When you use Mobile Voice Access over SIP trunks or H.323 gateways, you must enable the following settings on the trunk or gateway in Cisco Unified Communications Manager Administration:

- For SIP trunks, you must check the **Redirecting Diversion Header Delivery - Inbound** check box in the Trunk Configuration window.
- For H.323 gateways, you must check the **Redirecting Number IE Delivery - Inbound** check box in the Gateway Configuration window.

CSCts21965 Troubleshooting When You Lose Both Security Tokens (Etoken)

Tip Perform the following procedure during a scheduled maintenance window because you must reboot all servers in the cluster for the changes to take effect.

If you lose the security tokens and you need to update the CTL file, perform the following procedure:

Procedure

Step 1 On every Cisco Unified CallManager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists using the CLI command *file list tftp CTLFile.tlv.*

Step 2 Delete CTLFile.tlv using the CLI command *file delete tftp CTLFile.tlv.*

Step 3 Repeat Step 1 and Step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 Use the Cisco CTL client to create the CTL File. (For information on creating a CTL file, see *Cisco Unified Communications Manager Security Guide*.)

Tip Use the Cisco CTL client to create the CTL File. (For information on creating a CTL file, see *Cisco Unified Communications Manager Security Guide*.)If the clusterwide security mode exists in mixed mode, the Cisco CTL client displays the message, “No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click **OK**; then, choose **Set CallManager Cluster to Mixed Mode** and complete the CTL file configuration.

Step 6 After you create the CTL file on all the servers, delete the CTL file from the phone. (For information on deleting a CTL file, see *Cisco Unified Communications Manager Security Guide*.).

Step 7 Reboot all the servers in the cluster.

CSCtr07539 MDCX Sendonly Message Suppressed for MGCP Calls

For all MGCP calls, Cisco Unified Communications Manager suppresses the media layer from sending any MDCX (M:sendonly) messages to the MGCP gateway. This is done to prevent one-way audio scenarios.

CSCtf48747 DTMF Suppressed When G.Clear is Advertised

Cisco Unified Communications Manager suppresses DTMF configuration settings for all calls on which G.Clear is advertised in the list of codecs, irrespective of whether G.Clear is chosen as the codec for the call.

CSCte44108 Call Control Discovery Limitation

The following information is missing from the "Call Control Discovery" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

CCD has a limitation with three clusters (A, B and C), when C learns the advertisements of A and B.

In this scenario, when two clusters (A and B) are present, both of them advertise the same pattern, and cluster B advertises later than cluster A. This behavior overwrites the PSTN failover rule for cluster A which cluster C adopts. If your IP connection is lost, calls from cluster C are always redirected to cluster B via PSTN.

After you delete the cluster B advertisement, the PSTN failover rule still points back to A. If your IP connection is lost, calls from cluster C are redirected to cluster A via PSTN.

CSCtx00678 Do not use Voicemail for Alerting Name or ASCII Alerting Name

Do not use the word "Voicemail" anywhere in the Alerting Name or ASCII Alerting Name fields in the Directory Number Configuration window. If you use the word "Voicemail" Cisco Unity Connection may process the call as a direct call rather than as a forwarded call.

CSCtx86215 Database Replication

This section of the Cisco Unified Communications Manager System Issues chapter in the *Troubleshooting Guide for Cisco Unified Communications Manager* requires this addition:

Extension Mobility does not work when database replication breaks between the Unified CM node running Extension Mobility and the Unified CM node to which the phone is registered.

CSCtr82936 Not able to add an IPSEC Policy Group Name or a Policy Name with two hyphens

When you are creating a name for Policy Group Name or Policy Name in Cisco Unified Communications Manager OS Administration under **Security -> IPSEC Policy** configuration, and enter a name with two hyphens you get an error that the name is invalid. Do not use more than one hyphen when creating the Policy Group Name or Policy Name.

CSCtc71174 Call Park and Directed Call Park Restriction

The following call flow shows a limitation with the Call Park and Directed Call Park features.

1. Phone A calls Phone B.
2. Phone B parks the call. Phone A is now connected to MOH.
3. Phone A presses Hold (Mutual Hold).
4. Phone C dials the parked number through a H323 Trunk.
5. No audio is produced and the call fails after 12 sec (MXTimeout).

In this call flow, when you retrieve a parked call across an H323 ICT that is also on hold, the call fails. By the time phone C tries to retrieve the parked call, the parked party is on hold and Unified CM cannot cut through media.

CSCuc10415 Tip for Adding a New Server

The following tip needs to be added to the "Server settings" topic in the *Cisco Unified Communications Manager Administration Guide.*

To avoid errors, Cisco recommends that you add a server to the system with a name that has less than 47 characters. Then, update the server name to the target length.

CSCuc77135 Port Information for UDS

The *Cisco Unified Communications Manager TCP and UDP Port Usage* document does not mention port usage information for Cisco User Data Services. Endpoints can make a TCP connection to Cisco Unified Communications Manager port 8443 for Cisco User Data Services requests.

CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none>

The following note is missing from the "Phone Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool.

CSCtw44980 Missing Exceptions for Voice-Mail Pilot

The following information is missing for the Voice Mail Pilot Name field description in the "Voice-Mail Pilot Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#).

CSCud34740 Application User AXL Password Must Not Contain Special Characters

The following note is missing from the Application User Settings topic in the Cisco Unified Communications Manager Administration Online Help:

Note Do not use special characters when you create an AXL password for an application user.

CSCud57169 CTL file size limit of 32 kilobytes should be 64 kilobytes

The *Cisco Unified Communications Manager Security Guide* states that "The Cisco CTL Client limits the file size of a CTL file to 32 kilobytes because the phones cannot accept a larger CTL file."

The file limit should state 64 kilobytes.

CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide

The *Cisco Unified Communications Manager Troubleshooting Guide* is missing the following procedure for troubleshooting if you lose all security tokens (etokens):

Perform the following procedure if you lose the security tokens and you need to update the CTL file.

Tip Perform the following procedure during a scheduled maintenance window, because you must reboot all servers in the cluster for the changes to take effect.

Step 1 On every Cisco Unified CallManager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists from the OS SSH command line.

file list tftp CTLFile.tlv

Step 2 Delete CTLFile.tlv.

file delete tftp CTLFile.tlv

Step 3 Repeat step 1 and step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 By using the Cisco CTL client, create the CTL File, as described in "Installing the Cisco CTL Client" and "Configuring the Cisco CTL Client".

Tip If the clusterwide security mode is in mixed mode, the Cisco CTL client displays the message No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click OK; then, choose Set CallManager Cluster to Mixed Mode and complete the CTL file configuration.

Step 6 Reboot all the servers in the cluster.

Step 7 After you create the CTL file on all the servers and reboot all servers in the cluster, delete the CTL file from the phone, as described in "Deleting the CTL File on the Cisco Unified IP Phone".

CSCuc62305 Documenation for CDR CallingPartyNumber for Callpickup and Transfer case

When the Service Parameter Auto Call Pickup Enabled is set to True for an IP Phone and a Cisco Unified Communications Manager receives an incoming call that the IP phone picks up, the prefix digit defined in the Translation Pattern is added to the callingPartyNumber in CDR. However, the prefix digit is not added when the Service Parameter Auto Call Pickup Enabled is set to False. The prefix digits defined in the Translation Pattern only applies to basic call.

CSCud87708 Audit Log Severity Levels

The following table displays descriptions for audit log severity levels. Audit logs are accessed in Cisco Unified Serviceability.

Severity Code	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

CSCui20049 Restructure of Disaster Recovery Documentation for Restore Scenarios

Restore Scenarios

Caution Be aware that DRS encryption depends on the cluster security password. If you have changed the security password between the backup and this restore, DRS will ask for the old security password. Therefore, to use such old backups, you must remember the old security password or take a backup immediately after the security password change/reset.

You can restore Cisco Unified Communications Manager in the following scenarios:

- Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild), page 47
- Restoring the First Node only (Rebuilding the Publisher Alone), page 50
- Restoring the Entire Cluster, page 52
- Restoring Subsequent Cluster Nodes (With or Without Rebuild), page 54

Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)

Note Use this procedure only if you are restoring the node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure. If you intend to rebuild the publisher server, read the "Restoring the First Node only (Rebuilding the Publisher Alone)" section on page 50. If you intend to rebuild the entire cluster, read the "Restoring the Entire Cluster" section on page 52.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 7.0(**1**).1000-1 to version 7.1(**2**).1000-1, or from version 7.1(2).1000-**1** to version 7.1(2).1000-**2**. (The last parts of the version number change when you install a service release or an engineering special.) In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unified Communications Manager database restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore.

The Restore Wizard walks you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 4 Choose the backup device from which to restore in the **Select Backup Device** area. Then, click **Next**.

The Restore Wizard Step 2 window displays.

Step 5 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 6 Click **Next**. The Restore Wizard Step 3 window displays.

Step 7 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 8 Click **Next**. The Restore Wizard Step 4 window displays.

Step 9 Select the **Perform file integrity check using SHA1 Message Digest** checkbox if you want to run a file integrity check.

Note The file integrity check is optional and is only required in the case of SFTP backups. You do not need to run a file integrity check when restoring from tape and local device backups.

Note Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which considerably slows down the restore process.

Step 10 When you get prompted to choose the node to restore, choose the appropriate node.

Step 11 If the node that you chose is a publisher node, from the Select Server Name drop-down list box, choose the subscriber node from which you want to restore the publisher database. The Disaster Recovery System restores all nondatabase information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component and if the node that you chose is a publisher node.

Step 12 To start restoring the data, click **Restore**.

Note If you selected the **Perform file integrity check using SHA1 Message Digest** checkbox in Step 9, DRS runs a file integrity check on each file when you click **Restore**. If the system finds discrepancies in any .tar file during the check, the restore process will ERROR out the component that failed the integrity check and move to restore the next .tar file (that is, the next component).

Caution After you choose the node to which you want the data restored, any existing data on that server gets overwritten.

Note If you choose the first node to restore the data, DRS automatically restores the Cisco Unified Communications Manager database on the subsequent nodes. Read "Restoring the First Node only (Rebuilding the Publisher Alone)" section on page 50 for more details.

Step 13 Your data gets restored on the node that you chose.

Step 14 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions. The value on each node should be equal 2.

Note Database replication on the subsequent nodes may take enough time to complete depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication reset" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 15 If the database replication status is 2, restart the server. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

Note If you are restoring only to the first node, you must restart all nodes in the cluster. Make sure that you restart the subsequent node(s) before you restart the first node.

Note When the subsequent node(s) has restarted and is running the restored version of Cisco Unified Communications Manager, restart the first node.

Restoring the First Node only (Rebuilding the Publisher Alone)

Follow this procedure to restore the first node or publisher server in the cluster.

Procedure

Note Cisco recommends that you perform a fresh installation of Cisco Unified Communications Manager on the first node. For more information on installing Cisco Unified Communications Manager, see *Installing Cisco Unified Communications Manager*.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1.(2).1000-1 to version 6.1(2).1000-2.

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore.

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Configure the backup device.

Step 4 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 5 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 6 Click **Next**. The Restore Wizard Step 2 window displays.

Step 7 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 8 Click **Next**. The Restore Wizard Step 3 window displays.

Step 9 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 10 Click **Next**. The Restore Wizard Step 4 window displays.

Step 11 When you get prompted to choose the nodes to restore, choose only the first node (the publisher).

Caution Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

Step 12 (Optional) From the Select Server Name drop-down list box, choose the subscriber node from which you want to restore the publisher database. The Disaster Recovery System restores all nondatabase information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 15 and restore the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Note Make sure the subscriber node that you chose is up and connected to the cluster. A subscriber node can be added manually tothe cluster in Cisco Unified Communications Manager Administration (System > Server).

Step 13 To start restoring the data, click **Restore**.

Step 14 Your data gets restored on the publisher node.

Step 15 During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Note Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored.

Note Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 16 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions. The value on each node should be equal 2.

Note Database replication on the subsequent nodes may take enough time to complete depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication reset" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 17 If the database replication status is 2, restart the server. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

Note If you are restoring only to the first node, you must restart all nodes in the cluster. Make sure that you restart the subsequent node(s) before you restart the first node.

Note When the subsequent node(s) has restarted and is running the restored version of Cisco Unified Communications Manager, restart the first node.

Restoring the Entire Cluster

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you may need to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster:

Tip If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform the following procedure.

Note You can restore the whole cluster as a single operation after you rebuild the publisher server and the subscriber servers, or to revert to a known good configuration. You do not need to restore the first node and the subsequent nodes in two separate operations.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Note Before you restore a cluster, make sure that all nodes in the cluster are up and communicating with the first node. You must perform a fresh install for the nodes that are down or not communicating with first node at the time of the restore.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Configure the backup device.

Step 4 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 5 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 6 Click **Next**. The Restore Wizard Step 2 window displays.

Step 7 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 8 Click **Next**. The Restore Wizard Step 3 window displays.

Step 9 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 10 Click **Next**. The Restore Wizard Step 4 window displays.

Step 11 When you get prompted to choose the nodes to restore, choose all the nodes in the cluster.

Note The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

Note If a subsequent node is down or not connected to the cluster during the cluster restore, the database component restore will skip that node and proceed with the next one. You must perform a fresh install of Cisco Unified Communications Manager on these subsequent nodes.

Step 12 Your data gets restored on all the nodes of the cluster.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Note Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 13 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, Check the Replication Status value on all nodes by using the "utils dbreplication runtimestate" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions. The value on each node should be equal 2.

Note Database replication on the subsequent nodes may take enough time to complete depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication reset" CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 14 If the database replication status is 2, restart the server. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

Note If you are restoring only to the first node, you must restart all nodes in the cluster. Make sure that you restart the subsequent node(s) before you restart the first node.

Note When the subsequent node(s) has restarted and is running the restored version of Cisco Unified Communications Manager, restart the first node.

Restoring Subsequent Cluster Nodes (With or Without Rebuild)

Follow this procedure to restore subsequent nodes in the cluster.

Note Extension Mobility Cross Cluster users who logged in to a remote cluster at backup shall remain logged in after restore.

Procedure

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1.(2).1000-1 to version 6.1(2).1000-2.

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, and deployment type of the restore matches the hostname, IP address and deployment type of the backup file that you want to restore.

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Note If you are restoring the subsequent nodes after a rebuild, you must configure the backup device. For more information, see Managing Backup Devices, page 6.

Step 3 Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1window displays.

Step 4 In the **Select Backup Device** area, choose the backup device from which to restore.

Step 5 Click **Next**. The Restore Wizard Step 2 window displays.

Step 6 Choose the backup file that you want to restore.

Caution If you restored the first node earlier, you must choose the same backup file that you used to restore the first node to restore subsequent nodes in the cluster.

Step 7 Click **Next**. The Restore Wizard Step 3 window displays.

Step 8 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 9 Click **Next**. The Restore Wizard Step 4 window displays.

Step 10 When you get prompted to choose the nodes to restore, choose only the subsequent nodes.

Step 11 To start restoring the data, click **Restore**. Your data gets restored on the subsequent nodes.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Step 12 When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, restart the server. For more information on restarting, see the Cisco Unified Communications Operating System Administration Guide.

New and Changed Information

The *New and Changed Information for Cisco Unified Communications Manager 8.6(2)* provides information about new and changed features for release 8.6(2).

To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/8_6_2/delta/delta862.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(2) 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(2) as of September 29, 2011 describe possible unexpected behaviors in Unified CM Release 8.6(2), 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(2) as of September 29, 2011" section on page 59 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(2) as of September 29, 2011" section on page 59 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 56.

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(2) as of September 29, 2011

The following table lists open caveats which may cause unexpected behavior in Unified CM 8.6(2).

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011

IDENTIFIER	COMPONENT	HEADLINE
CSCtq94673	cp-sip-station	CUCM core dump when SIP phone deregisters during a call
CSCts32087	cmcti	CFC #5489 - JTAPI connect command (Make Call) generates Exception
CSCts32768	cp-mediacontrol	DVOR full call model, call dropped with SIP & same problem on EO DVOR
CSCtr83193	cp-subscriptionmgr	RL fails after SDLLinkOOS with node on which trunk is registered
CSCts40785	sa-callp	BE3K:Displays an error message for the localized sites name
CSCto57427	cpi-os	Cannot ping ipv6 addresses outside its own subnet from 8.6 UCM
CSCts00471	cp-mediacontrol	cBarge_call_dropped with E2E rsvp
CSCtr51605	cmcti	Register/Unregister event on old device passed when EM login NCD
CSCts05068	sa-callp	Unable to make emergency call from Remote site in INNP
CSCts05617	ims	SSO configs are not migrated after L2/RU w/ having ccmadmin sso disabled
CSCts23810	voice-sipstack	Unified CM does not forward ACK on tandem SIP to SIP call flow
CSCtj73909	cpi-os	Tomcat core during restore and java core during RU including RU COP
CSCtr79913	cp-mediacontrol	Media Negotiation Failure on EO SIP Trunk Call with Multiple SRTP Codec
CSCts31310	sa-mac	CDR does not display the date more then 50 record
CSCtr81497	cmcti	Wrong dev caps on RT-lite when device is reset

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011 (continued)

CSCtf37698	cmcti	Incorrect reason code in ExistingCallEvent for supervisor
CSCts33393	ccmcip	Calls fail to endpoints with long directory number.
CSCts33408	jtapisdk	Fail to get CreatedEv for park number when unpark call with SP true
CSCts33572	cpi-appinstall	U1 Upgrade:Remove extra Error Screen which appears before second reboot
CSCts34379	cmui	CUCM portal may reveal if a username exists
CSCts34483	cp-mediacontrol	Not able to make inter cluster(H323 Trunk) call between two H323 EP
CSCtr83175	ccm-serviceability	SCH : Alerts are not generated by Sub during fail over
CSCts34511	sa-mac	CDR off loading help page is blank
CSCts34664	cp-sip-station	3rd Party SIP phones unable to register post Upgrade to 7.1.5.32021-1
CSCtk32432	cpi-third-party	Update TPL OpenSSL to Addresss Published Vulnerabilities
CSCts28932	cp-mgcp	CUCM not disconnecting calls when ip phone gets disconnected
CSCts35174	cpi-appinstall	RU 8.5(1) to 8.6(1) fails on 782xH3 when N/W Fault Tolerance enabled
CSCts01512	axl	AXL query returns duplicate rooms/phones for ctsman querry
CSCts36156	cmcti	Incorrect reason code in DeviceUnRegisterEvent and DeviceRegisterEvent
CSCtr85979	ccm-serviceability	axl service activation automation fails in 8.6.2.10000-1
CSCtn08912	database-ids	PMR 86128 corrupt syscdr resulting in bogus error 62 and/or 92
CSCtn13200	sa-fxn	When DSP is configured with a new IP, old IP is still pingable
CSCts37066	sa-mac	Save success msg doesnt display after modified system Date/Time setting
CSCts37102	sa-mac	IE8:ClicksonPage Naviga.button inCDR-CallDetails Page takes toHomescreen
CSCts37516	sa-callp	FTS pages for the new features are not localized
CSCts35340	cmcti	IPV6_CTI_35a: Fail to get TermRegistrationFailedEv after change RP mode
CSCts39201	cp-mobility	Subscriber incorrectly indicates NumRegisteredDevices is exceeded
CSCts39424	cm-docs	CUCM - MGCP Gateway Documentation html page - Not linked

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011 (continued)

CSCts39482	ccm-serviceability	Cisco Reporter Service is not listed in the Control Center-Features Page
CSCtn99179	cp-mediacontrol	Call gets disconnected when EX90 to 7985 call is Transferred over EO.
CSCtr87743	licensing	First time upgrade failed after migration to FCS Volaris server
CSCts39130	sa-mac	reach me anywhere check box appears then disappears on user page
CSCts37514	sa-callp	Aus Country Pack- Announcemnts are in US Eng instead of Aus Eng
CSCto09866	cmcti	Unable to create conference chain with Codian Conference Bridge
CSCto10917	cp-mediacontrol	H245Interface trigger DTMFProfileChanged for H323 to H323 call
CSCts40968	sa-platform	cucmbe3k and classic installation fails on mcs-7816-i5 unrst builds
CSCtn75242	cpi-appinstall	RU: Add Email Notification to GUI
CSCts41204	cp-sccp	SCCP video calls from CUPC is not working
CSCts41251	cp-mobility	Phone2 CFA to its VM, NurD call to its shared mobile2 hits call fail
CSCtr89154	cp-mediacontrol	CM 8.5.1 - Ignores new port info even when new SIP conn id in reINVITE
CSCts41505	sa-spa	Attendant Group not working with SPA FXS updates.
CSCts41849	sa-callp	Volaris Blind Transfer of PSTN T1 CAS call back to PSTN fails
CSCtr90951	rtmt-dp	CUCMBE License information failed to generate in RTMT
CSCtr41885	cmcti	Dont receive DeviceUnRegisterEvent after EMlogin and wrong reason code
CSCtr91719	rtmt	FTP for RTMT Scheduled Trace Collection Not Ending Packet with CRLF
CSCtr94061	cpi-appinstall	Cucm 8.5.1 install fails with a timer expiry
CSCto86857	cp-mediacontrol	A transferred call with trp cannot be resumed for this case
CSCtr99004	cp-mediacontrol	SCCP---MTP----SIP(EO) : SCCP doesnt do OLC with correct payload.
CSCto92223	cmcti	ChangedParticipantNumber is empty in CCSCE after transfer and conf chain
CSCto94883	sa-gateway	Notify user to configure Cisco ISR2901 at end of PSTN Connection Wizard
CSCtq79475	cp-mobility	Cisco Jabber for Android client is unable to register

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011 (continued)

CSCts00137	cmui	Cius UPP: Allowed or Blocked List cant remove member filter
CSCts00260	cp-mediacontrol	410kbps has been reserved for video stream in video conference
CSCtq00929	sa-emergency	CUCMBE3k - Emergency call fails DA cache not rebuilt after restart
CSCts00299	cp-mediacontrol	Telepresence audio bandwidth modified to low value
CSCtq01514	cp-sip-trunk	Additional Characters in SDI logs when a call made via QSIG SIP Trunk
CSCts02176	database	libdbl.so keeps ccm from terminating gracefully
CSCtr51441	cmui	Applying COP file via the UI hangs permanently
CSCts03066	cp-sip-trunk	Agent greeting call failure during load with CCM861
CSCtr52906	cp-sip-trunk	ETSGJ-CH: "Private" displays on the Calling Party instead of Conference
CSCtq19020	database-ids	PMR 04791 Assert during out of memory testing on 55GB virtual server
CSCtq91607	selinux	"utils firewall ipv4 disable" command not working-SELinux in enforcing
CSCts06233	security	Racoon issue in RHEL5 with fresh upgrade
CSCtc59039	licensing	CLI file delete licensing doesnt remove DB entries in licenseinfo
CSCtr56948	cp-ss-callpark	Parked Number is showing in ENGLISH language instead of JAPANESE
CSCts09977	security	TVS can not authenticate 7.1(3) UCM certitiicate
CSCtr59256	cp-qsig	QSIG Path replace fails after CUCM detects PRPropose collision
CSCto97489	cpi-os	Post-upgrade reboot halts due to hp-health process failing to shut down
CSCts13318	database	CMDB does not handle Alarm 47 correctly
CSCts17913	cp-sip-station	Ringback tone heard on 8961 Phones is different(quick rings)over gateway
CSCtr05580	cpi-os	System locked out forever and restart not allowed for pwrecovery in RU
CSCto95557	ccm-serviceability	Audit Administrator user, couldnt able to edit Audit Log Configuration
CSCtr09671	cpi-appinstall	2TB USB drive cannot be detected for 25H3 RU from 8.5.1 to MB for CUC
CSCtq80906	ccm-serviceability	New user with System Administrator role not able to view "Audit Log"

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011 (continued)

CSCtl44970	database-ids	PMR 84047 Assert Failure read_record: unexpected log record type 11.50.
CSCtr65692	sa-mac	after adding ssh info, still can;t ssh to phones
CSCts22512	selinux	utils import config fails to change the os admin username and password.
CSCts23528	cp-ss-callpark	Call Park retrieve failures when original CP code mgr returns online
CSCtr69193	ccm-serviceability	Trace is generated even when the trace is set to off for BPS and TAPS
CSCtr78976	ccmcip	Secured Directory URL repopulates to default URL upon cucm reboot
CSCts24439	cmcti	No response on EO GET_IP_PORTrequest on CTIport with static registration
CSCts24527	cmui	CCMAdmin find list table is missing when search contains a VG phone
CSCts24666	cp-mobility	"Ignore Call Forward All on Enterprise DN" definition example reversed
CSCtr73191	cpi-os	Connectivity test may fail during initial subscriber install for CUCM
CSCtr19541	sa-maintenance	License Report pageon CUCMBE3K doesnt display statusof installed license
CSCtr75944	cp-mediacontrol	SIPv6 GW calling over SIPv4 to SCCPv6 fails
CSCtr76109	cmcti	LastRedirectPartyName is incorrect in CPIC after IVR answer call
CSCtr72226	sa-docs	trouble shooting page doesnt open when system volatge goes out of thresh
CSCtq48318	sa-gateway	PSTN Gateway port 1 is out of service
CSCts27537	cmcti	Get Term/Address outofservice and registration fail on register CTI port
CSCts27621	cmcti	Supervisor (CTI port) WC call dropped out when CCM failback
CSCtr78782	cp-mediacontrol	H.323 Calling over SIPv4 ICT to SCCPv6 fails
CSCts29204	cp-sip-trunk	Caller ID from SIP trunk is blank if Contact field contains no number
CSCtr23190	cpi-security	IPSEC via Certificates
CSCtr79960	sa-localpstn	CDR record type for emergency number is showing as ON Net
CSCts30604	bps-bat	UDP BAT template changes device name case
CSCtr80063	cp-mediacontrol	LS sip video not seen during CUVC meetme conference
CSCts30850	sa-day1wizard	IE8:FTS:5XX Server Error:VerifyServerSideSetup when does Assume Control

Table 8 Open Caveats for Unified CM Release 8.6(2) as of September 29, 2011 (continued)

CSCts31243	sa-day1wizard	FTS: Unable to upload spreadsheet with default PSTN Gateway Settings
CSCts35326	cpi-os	"KERNEL: assertion (!sk->sk_forward_alloc) failed at net/ipv4/af_inet.c (152)" displayed on console screen
CSCtr84167	cm-docs	Unity blind transfer with block offnet to offnet transfer enabled
CSCtr21486	cm-docs	When there is a version mismatch between a subscriber server and publisher server, the Cisco Unified Communications Manager history file does not log a switch version entry.

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 Cisco Unified Communications Manager

The following changes exist for the Unified CM 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.

Device Name and Description fields need to be updated

In the Unified CM Administration menu **Device > Trunk**, the Device Name and Description fields should read as follows:

Field	Description
Device Name	Enter a unique identifier for the trunk. The device name can include up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only.
Description	Enter a descriptive name for the trunk. The description can include up to 114 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

CSCug38337 TFTP Service Parameter "Maximum Serving Count"

The online help for the TFTP maximum serving count, which specifies the maximum number of client requests to accept and to serve files at a time, should be 3000 and not 5000 as currently listed.

Missing Field in E & M Port Configuration Settings

The E & M Port Configurations section of the Gateway Configuration chapter in the Cisco Unified Communications Manager Administration Guide is missing the Unattended Port field description. Users should check the Unattended Port check box to indicate the device is attached to an unattended port, such as a voice mail port.

Cisco Unified Communications Manager Call Detail Records Administration Guide

The following changes exist for the Call Detail Records Administration documentation:

- Codec Types, page 65
- CDR Field Descriptions, page 66

Codec Types

The Codec Types table in Chapter 6 of the Cisco Unified Communications Manager Call Detail Records Administration Guide is missing the entries in the following table.

Table 9 Codec Types

Value	Description
97	AMR Codec
98	AMR-WB Codec

CDR Field Descriptions

The CDR Field Descriptions table in the Cisco Call Detail Records Field Descriptions chapter contains errors and omissions relating to video codecs and video resolution fields. The following table shows the corrections:

Table 10 CDR Field Descriptions

Field	Range of Values	Description
origVideoCap_Codec	0, 100 = H.261, 101 = H.263, 103 = H.264	This field identifies the codec type that the originator uses to transmit video (H.261, H.263, or H.264.) Default - 0. If media is not established, this field stays 0.
origVideoCap_Resolution	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution 7 = W360P 8 = VGA 9 = W448P 10 = HD720P 11 = HD1080P 12 = CIF2	This field indicates the transmitting resolution. In the case of H.264 codec or SIP device, this field refers to the max transmitting resolution the device can transmit for this call. Default - 0. If media is not established, this field stays 0.
destVideoCap_Codec	0, 100 = H.261, 101 = H.263, 103 = H.264	This field identifies the codec type that the terminating party uses to transmit video (H.261, H.263, or H.264). Default - 0. If the destination cannot be reached, this field stays 0.

Field	Range of Values	Description
destVideoCap_Resolution	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution 7 = W360P 8 = VGA 9 = W448P 10 = HD720P 11 = HD1080P 12 = CIF2	This field indicates the transmitting resolution. In the case of H.264 codec or SIP device, this field refers to the max transmitting resolution the device can transmit for this call. Default - 0. If media is not established, this field stays 0.
origVideoCap_Codec_ Channel2	0, 100 = H.261, 101 = H.263, 103 = H.264	This field identifies the codec type that the originator uses to transmit video (H.261, H.263, or H.264) for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
origVideoCap_Resolution_Channel 2	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution 7 = W360P 8 = VGA 9 = W448P 10 = HD720P 11 = HD1080P 12 = CIF2	This field indicates the transmitting resolution for the second video channel. In the case of H.264 codec or SIP device, this field refers to the maximum transmitting resolution the device can transmit for this call. Default - 0. If media is not established, this field stays 0. Also, if H.239 is not supported, this field displays 0.

Field	Range of Values	Description
destVideoCap_Codec_Channel2	0, 100 = H.261, 101 = H.263, 103 = H.264	This field identifies the codec type that the terminating party uses to transmit video (H.261, H.263, or H.264) for the second video channel. Default - 0. If the destination cannot be reached, this field stays 0.
destVideoResolution_Channel2	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution 7 = W360P 8 = VGA 9 = W448P 10 = HD720P 11 = HD1080P 12 = CIF2	This field indicates the transmitting resolution for the second video channel. In the case of H.264 codec or SIP device, this field refers to the maximum transmitting resolution the device can transmit for this call. Default - 0. If media is not established, this field stays 0. Also, if H.239 is not supported, this field displays 0.

Cisco Unified Communications Manager Features and Services Guide

The following changes exist for the *Cisco Unified Communications Manager Features and Services Guide*:

- Block Offnet to Offnet Transfer Information is Missing, page 68
- Remote Cluster Menu Path is Incorrect, page 69
- Configure BLF Call Pickup, page 69

Block Offnet to Offnet Transfer Information is Missing

The following text is missing from the "External Call Transfer Restrictions" chapter in *Cisco Unified Communications Manager Features and Services Guide*.

When you enable the service parameter Block Offnet to Offnet Transfer and make a blind transfer with Cisco Unity Connection, the Q.931 SETUP message which Cisco Unified Communications Manager sends to the PSTN gateway for an outbound PRI call still reaches the gateway. This transfer results in a dropped call.

Remote Cluster Menu Path is Incorrect

In the Remote Cluster Configuration section of the "EMCC Configuration" chapter of *Cisco Unified Communications Manager Features and Services Guide*, the menu path **Advanced Features > EMCC > EMCC Remote Cluster** is incorrect and should be **Advanced Features > Cluster View**.

Configure BLF Call Pickup

Step 10 of the Configure BLF Call Pickup is an optional step that instructs users on how to configure the Cisco Support Use 1 enterprise parameter. This step and this enterprise parameter are no longer needed to configure BLF call pickup.

Command Line Interface Reference Guide for Cisco Unifed Communications Solutions

The following information about **utils auditd** is missing from the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*:

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Cisco Unified Communications Manager Administration Guide

The following change exists for Cisco Unified Communications Manager Administration Guide:

CSCuh62299 Note added to the Service Name field, page 69

CSCuh62299 Note added to the Service Name field

The following note is added to the Service Name field under IP phone service settings table in the Cisco Unified Communications Manager Administration Guide.

Note When the service URL points to an external customized URL, you cannot localize the service name as per the device locale of the phone. The service name gets displayed in English alphabets only.

Cisco Unified Communications Manager System Guide

The following changes exist for the Cisco Unified Communications Manager System Guide:

- CSCue75498 Understanding Cisco Unified Communications Manager Trunk Types, page 70

CSCue75498 Understanding Cisco Unified Communications Manager Trunk Types

Step 10 of the Trunk Configuration Checklist in the Cisco Unified Communications Manager System Guide states "When you enable Send send-receive SDP in mid-call INVITE for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line." This statement incorrectly qualifies the situation as occurring in tandem mode only. This situation can occur for all clusters.

Cisco Unified Communications Manager TCP and UDP Port Usage Guide

The following TCP port description is missing from the Port Descriptions table in *Cisco Unified Communications Manager TCP and UDP Port Usage Guide*::

From (Sender)	To (Listener)	Destination Port	Purpose
Unified CM (Tomcat)	Unified CM (Tomcat)	8080 / TCP	Communication between servers used for diagnostic tests

Cisco Unified Serviceability Administration Guide

The Cisco Unified Serviceability Administration Guide contains the following updates:

- CSCud87708 Audit Log Severity Levels, page 70

CSCud87708 Audit Log Severity Levels

The following table displays desciptions for audit log severity levels. Audit logs are accessed in Cisco Unified Serviceability.

Severity Code	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical condition
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significat condition
6	Informational: informational messages
7	Debug: debug-level messages

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.