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

January 14, 2016

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(1a) Release Notes

Date	Changes
6-22-16	Added Outdated Information for Auto-Attendant, page 65
3-11-16	Added Directory Number Field Description Updated, page 80
2-02-16	Added Domain Name Change for Cisco Unified Communications Manager, page 79.
1-14-16	Added Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 30.
7-21-15	Added Correction in Software Conference Bridge Maximum Audio Streams, page 90.
6-30-15	Added Correction in Software Conference Bridge Maximum Audio Streams, page 90.
4-14-15	Added FAC and CMC Code is not Captured in CDR, page 84.
4-13-15	Added CSCus63274 Devices Reset After Certificate Regeneration, page 97.
3-10-15	Added Incorrect Order of CDR and CMR Fields, page 83.
2-16-15	Added Incorrect CDR Field Description for destCallTerminationOnBehalfOf, page 83.
1-8-15	Added Supported SFTP Servers to System Requirements, page 4.
12-16-14	Added Missing Information about TCP Port 22, page 92
11-04-14	Added Incorrect Note about User Locales, page 91.
10-07-14	Added Missing Information about the Platform Administrative Web Service, page 93.

Cisco Systems, Inc.
www.cisco.com

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

Date	Changes
9-19-14	Added show perf query counter Command Output, page 101.
9-5-14	Added Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert, page 100.
8-26-14	Added CSCup45037 Transmit UTF8 for Calling Party Name Field Correction, page 91.
7-16-14	Added CSCup71020 MaxReturnedDevices in Serviceability XML, page 65
6-27-14	Added Configuring OpenAM Section, page 88and CSCtd43582 Remote Destination and Auto Answer, page 65.
6-3-14	Added CSCup04321 Call Pickup Group Visual Notification does not Support Localization, page 64.
5-16-14	Added CSCuo10697 Updated List of LDAP Supported Directories.
4-30-14	Added CSCum01216 Serviceability XML API doc in error, page 30 and CSCuo13148 Cisco ATA 187 Analog Telephone Adaptor Compatibility.
4-7-14	Added CSCuo01831 Phone Models Supporting Encrypted Configuration File to Cisco Unified Communications Manager Security Guide, page 95
3-27-14	Updated Overview of the Software Upgrade Process, page 9.
3-17-14	Added CSCun47221 Note added to the CDR Repository Manager section, page 93.
3-13-14	Added CSCul78860 BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials, page 92 and CSCuj71412 Secure Call Monitoring and Recording Update, page 96.
3-7-14	Added CSCun32117- Bulk Certificate Import May Cause Phones To Restart, page 64 to Important Notes.
11-25-13	Added Cisco Unified Communications Manager TCP and UDP Port Usage, page 101 to Documentation Updates.
11-13-2013	Added Updated Caution to include DNS and Domain Name prior to restore, page 87 to Documentation Updates
10-15-13	Added Updates to section Phones that Support International Escape Character +, page 95 to Documentation Updates.
10-11-13	Added Added description for For voice mail usage option in Add hunt list procedure, page 91 to Documentation Updates.
09-25-13	Added note to upgrading pre-requisites about externally-powered USB.
08-30-13	Added Roll back cluster to a pre-8.0 release section update, page 96 to Documentation Updates.
08-29-13	Added CSCug84842 Installation fails with unrecoverable internal error, page 63 to Important Notes.
08-06-13	Added CSCui06050 Model is Not a Valid Device Field When Generation a Phone Report to Documentation Updates.
08-01-13	Added Cisco Unified Real-Time Monitoring Tool Administration Guide, page 100 to Documentation Updates.
07-31-13	Added CSCus63274 Devices Reset After Certificate Regeneration, page 97 to Documentation Updates.

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

Date	Changes
07-03-13	Added CSCuh62299 Note added to the Service Name field, page 91 to Documentation Updates.
06-19-13	Added Relabel of Use Personal Preferences field, page 90 to Documentation Updates.
06-03-13	Added Removed field Call Stats from SIP Profile configuration, page 90 to Documentation Updates.
04-24-13	Added CSCug36365 Call Park Display Timer restriction, page 30 to Important Notes.
04-09-13	Added CSCuf57901 Video resolution support for SIP phones, page 30 to Important Notes.
01-29-13	Added CSCub12922 Adding a new subscriber causes device reset, page 31 in Important Notes, page 27.
01-07-13	Added missing table entry for Redirect Reason Codes, page 83 to Documentation Updates.
01-04-13	Added CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 53 to Important Notes, page 27.
01-02-13	Added CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT, page 31 to Important Notes, page 27.

Contents

This document includes the following information:

- Introduction, page 4
- System Requirements, page 4
- Upgrading to Unified CM 8.6(1a), page 6
- Related Documentation, page 26
- Limitations and Restrictions, page 26
- Important Notes, page 27
- Caveats, page 65
- Documentation Updates, page 78
- Obtaining Documentation and Submitting a Service Request, page 102

Before you install or upgrade Cisco Unified Communications Manager (Unified CM), Cisco recommends that you review the "Upgrading to Unified CM 8.6(1a)" section on page 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.

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.

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

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

Uninterruptible Power Supply (UPS) Integration for Unified CM

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

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.

Supported SFTP Servers

Note We recommend that you retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. As a best practice, perform a backup and restore on a standby or backup server.

Use the information in the following table to determine which SFTP server solution to use in your system.

SFTP Server	Information
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade UCM for which versions compatible: https://marketplace.cisco.com
SFTP Server from another Third Party	These servers are third party provided, have limited Cisco testing, and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Upgrading to Unified CM 8.6(1a)

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

- Software Version Number, page 7
- Pre-Upgrade Tasks, page 7
- Software Upgrade Considerations, page 9
- Supported Upgrades, page 13
- Obtaining the Upgrade File, page 13
- Ordering the Upgrade Media, page 13
- Software Upgrade Procedures, page 14
- Post-Upgrade Tasks, page 20
- Resetting Database Replication When Reverting to an Older Product Release, page 22

- Installing COP Files, Dial Plans, and Locales, page 22
- Latest Software and Firmware Upgrades for Unified CM 8.6 on Cisco.com, page 26
- CSCtr11072 Music On Hold Audio File Upload May Be Slow Or May Fail To Upload, page 35

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

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

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

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

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 versions:

- Unified CM: 8.6.1.20000-1

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

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

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

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

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

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

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

- Before you upgrade a cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (publisher server) and subsequent nodes (subscriber servers). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.

- Before you perform the Cisco Unified Communications Manager upgrade, ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.
- After you complete the pre-upgrade tasks, review with the "Software Upgrade Considerations" section on page 9.

Software Upgrade Considerations

This section contains the following topics:

- Overview of the Software Upgrade Process, page 9
- Making Configuration Changes During an Upgrade, page 11
- Supported Upgrades, page 13

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 an externally powered 16GB USB device to facilitate data migration from the old system to the new installation. For Unity Connection and Business Edition 5000, a 128GB external USB device is required. It is recommended to use an externally powered USB drive as other drives may not be recognized during the Refresh Upgrade sequence.

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

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

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

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 is 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.

Note Install the software during off-peak hours or during a maintenance window to avoid impact from interruptions.

Note 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 may be lost. 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 After you install a new node in an existing cluster, all phones that are registered to the cluster are reset.

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

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

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

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

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

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

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

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

Step 5 Save changes.

Step 6 Restart the virtual machine.

Making Configuration Changes During an Upgrade

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

Administration Changes

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

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

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

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

Upgrade Tasks

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

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

Procedure

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

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

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

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

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

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

Step 5 Switch over subsequent nodes to the upgraded partition.

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

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

- In Cisco Unified Reporting, access the Unified CM Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0— Initializing.
  - 1—Replication setup script fired from this node.
  - 2—Good replication.
  - 3—Bad replication.
  - 4—Replication setup did not succeed.

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

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

User Provisioning

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

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

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

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

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

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

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

Software Upgrade Procedures

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

- Installing the COP File, page 14
- Upgrading to Restricted or Unrestricted Unified CM 8.6(1a), page 14
- Upgrading from a Local Source, page 15
- Upgrading from a Remote Source, page 16
- Supported SFTP Servers, page 17
- Bridge Upgrade, page 19

Installing the COP File

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

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

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

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

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

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

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

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

Procedure

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

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

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

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

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

For the restricted version:

1fffdad07be38d63bb64a29b821f0e0f UCSInstall_UCOS_8.6.1.20000-1.sgn.iso

For the unrestricted version:

f5fb68b8d99b0335bd1013eb1dad73e4 UCSInstall_UCOS_UNRST_8.6.1.20000-1.sgn.iso

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://developer.cisco.com/web/cdc/home

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 upgrade to Unified CM 8.6(1a), you must set the OS version to RedHat 5.5.

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
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, page 23
- Dial Plan Installation, page 23

- Locale Installation, page 23

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 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 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 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(1a) at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_6_1/rel_notes/ime-rel_notes-861.html.

Limitations and Restrictions

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

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

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

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

Important Notes

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

- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 30
- CSCum01216 Serviceability XML API doc in error, page 30
- CSCug36365 Call Park Display Timer restriction, page 30
- CSCuf57901 Video resolution support for SIP phones, page 30
- CSCub12922 Adding a new subscriber causes device reset, page 31
- CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT, page 31
- CSCuc39511 Expansion module field missing from certain device profiles, page 31
- CSCtb31860 Transcoding G.711 to All Codecs Supported, page 31
- CSCtr78911 Answer Too Late Timer, page 31
- CSCts83374 Remote Destination Configuration Settings for Single Number Reach and Reroute Remote Destination Calls to Enterprise Number, page 32
- CSCto57498 Upgrading to Cisco Unified Communications Manager Release 8.x from Release 7.x, page 32
- CSCtd69640 Downtime when upgrading Publisher server until all Subscriber servers are updated, page 33
- CSCtk68384 Disable ICH10 onboard SATA controller on EX/ESXi servers during Unified CM installation, page 34
- CSCub10861 Call waiting behavior with MLPP Preemption correction, page 34
- CSCua01779 Cisco Unified Communications Manager Locale Installer locale file for Belgium, page 34
- CSCtz88812 Cisco IP Phones and Cisco Unity Connection support for IPv6, page 34
- CSCte39796 Increase database replication timeout when upgrading large clusters, page 35
- CSCsy57492 Hold Reversion Notification Interval for SCCP and SIP phones, page 35
- New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651), page 35
- CSCtn32528 MLPP feature support only for SCCP phones, page 35
- CSCtr11072 Music On Hold Audio File Upload May Be Slow Or May Fail To Upload, page 35
- CSCtq96181 Cannot Add or Edit H323 Gateway on Device/Gateway Web Page, page 35
- Unrestricted Release Limitations, page 36
- New in User Options Page Beta, page 36

- CSCtq56727 SIP Gateway Crash During Heavy Call Traffic, page 37
- CSCtq84756 MCS 7835/45-I3 Server Freezes During Firmware Upgrade, page 37
- CSCtq47285 RingOut State Transfer or Hold, page 37
- Verify RAID Status Prior To Upgrade on 7825H3 and 7828H3 Servers, page 37
- CSCtq46578 iso file download error message, page 37
- CSCto31364 Cluster Fully Qualified Domain Name (CFQDN) Parameter, page 38
- CSCto83868 firmware update error message, page 38
- CSCtd87058 BAT Impact, page 38
- Call Park Feature Limitations, page 39
- CSCth53322 Rebuild Server After You Use the Recovery Disk, page 40
- CSCte05285 IBM I3 Servers Automatic Server Restart (ASR) Default Specifies Disabled, page 40
- CSCtd01766 Destination Port on Trunk Remains Unchanged After Upgrade, page 40
- CSCtl23382 Recovery CD Issues, page 41
- Disaster Recovery System Caution, page 41
- EMCC Login Affects Settings in Product-Specific Configuration Layout of Phone Configuration Window, page 42
- CSCtl47624 No Music On Hold when using ASR 1000, page 42
- CSCtq20098 To handle DRS Restore status monitoring in a scenario, page 42
- Limitations with Presentation Sharing when using a Cisco TelePresence MCU, page 43
- Video Conferencing with Cisco Integrated Services Routers Generation 2, page 43
- Interoperability with a Cisco TelePresence Video Communications Server, page 44
- CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value, page 45
- CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters, page 45
- CSCtr82936 Not able to add an IPSEC Policy Group Name or a Policy Name with two hyphens, page 45
- CSCtr89029 URL Parameters for Secured Phones Repopulated After Restart, page 46
- CSCtr62446 Route List Run on All Nodes Service Parameter, page 46
- CSCts13972 Must re-run CTL Client when the Domain Name Changes, page 46
- CSCtr84167 Block Offnet to Offnet Transfer, page 46
- CSCtr21486 Troubleshooting Guide Update to Switch Version, page 46
- CSCtg67435 Certificate Regeneration During Domain Name Change, page 46
- CSCtr54150 Mobile Voice Access over SIP trunks and H.323 Gateways, page 46
- CSCts21965 Troubleshooting When You Lose Both Security Tokens (Etoken), page 47
- CSCtr07539 MDCX Sendonly Message Suppressed for MGCP Calls, page 47
- CSCtf48747 DTMF Suppressed when G.Clear is Advertised, page 47
- CSCtw25693 MoH Does Not Support DTMF, page 47
- CSCte44108 Call Control Discovery Limitation, page 48
- CSCtx86215 Database Replication, page 48

- CSCty75069 Secured Directory URL Enterprise Parameter overrides Directory field in Phone Configuration, page 48
- CSCtr44481 Download Dial Plans for Cisco Unified Communications Manager Release 8.X, page 49
- CSCty16160 During publisher node restores DB replication status must be 2 before you reboot the cluster, page 49
- CSCtz83810 Directed Call Park MoH Audio Source Selection, page 49
- CSCtz73477 Interactions with Call Forward iDivert and Voice-Messaging features, page 49
- CSCtq03342 Loading of selload: SELinux process takes up 100% CPU on CUCM, page 49
- CSCtx86664 Port 6970 is open for HTTP requests to the TFTP server, page 49
- CSCtu52978 Hard disk replacement fails if write cache is enabled on Cisco MCS 7828/28-i3, page 50
- CSCtw79487 Default Device Pool may not be chosen after upgrades to 5.x or later, page 50
- CSCua75983 Support for midcall mobility features with Cisco Unified Border Element, page 50
- Failover/failback for dual mode phones, page 50
- CSCth80282 Update regenerate certificate in Unified CM Operating System Guide, page 50
- Secure shell password maximum length, page 51
- Only SIP re-INVITE is used for outbound transfers, page 51
- CSCtc71174 Call Park and Directed Call Park Restriction, page 51
- CSCub12688 FinalCalledPartyNumber CDR field description, page 51
- CSCub17607 SIP Redirect by Application requires a SIP route pattern, page 52
- CSCub59376 Missing step in procedure for updating Unified CM hostname, page 52
- CSCuc10415 Tip for Adding a New Server, page 52
- CSCuc23992 Call Preservation support for SIP trunks, page 52
- CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none>
- CSCtw44980 Missing Exceptions for Voice-Mail Pilot
- CSCud34740 Application User AXL Password Must Not Contain Special Characters, page 53
- CSCud57169 CTL file size limit of 32 kilobytes should be 64 kilobytes, page 53
- CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 53
- CSCui20049 Restructure of Disaster Recovery Documentation for Restore Scenarios, page 54
- CSCug84842 Installation fails with unrecoverable internal error, page 63
- CSCun32117- Bulk Certificate Import May Cause Phones To Restart, page 64
- CSCuo13148 Cisco ATA 187 Analog Telephone Adaptor Compatibility
- CSCuo10697 Updated List of LDAP Supported Directories, page 64
- CSCup04321 Call Pickup Group Visual Notification does not Support Localization, page 64
- CSCtd43582 Remote Destination and Auto Answer
- CSCup71020 MaxReturnedDevices in Serviceability XML
- Outdated Information for Auto-Attendant

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets

This information applies to CSCtn79567.

Cisco Unified IP Phones 7940 and 7960 do not support Cisco-signed Java Midlets, but they can parse the service information from the phone configuration file.

CSCum01216 Serviceability XML API doc in error

The following is implemented in Cisco Unified Communications Manager Release 10.0(1): The SelectCMDevice API returns SIP trunk status and also returns the IP addresses and status of the peer devices.

CSCug36365 Call Park Display Timer restriction

f you entered a Call Park Reversion Timer value that is less than the Call Park Display Timer, Call Park numbers may not display on the phone.

CSCuf57901 Video resolution support for SIP phones

Cisco Unified Communications Manager supports the imageattr line in the SDP portion of the SIP header for higher resolution video calls. Cisco SIP phones that support w360p (640 x 360), such as the 9951, 9971, and 8961, automatically select the best resolution for video calls depending on the following criteria:

- If the session level bandwidth is greater than 800Kb/s and the imageattr[640 x 480] line in the SDP exists, then VGA is used.
- If the session level bandwidth is greater than 800Kb/s and the imageattr[640 x 480] line in the SDP does not exist, then w360p is used.
- If the session level bandwidth is less than 800Kb/s but greater than 480 bits per second and the imageattr[640 x 480] line exists, then VGA 15 frames per second is used.

Note If you currently have a Cisco IP Phone model 9951, 9971, or 8961 that supports w360p (640 x 360) video resolution and are upgrading to Cisco Unified Communications Manager release 8.5(1) or later, you may notice changes in the resolution of video calls. The w360p resolution was introduced at phone load 9.2(1).

The following video call flow is between two 9951 phones (Phone A and Phone B) without imageattr line support (for example, using Cisco Unified Communications Manager releases 8.0(1) and earlier):

1. Phone A sends a SIP message with an imageattr line in the SDP.
2. Cisco Unified Communications Manager deletes the imageattr line in the SDP and then sends the modified SIP message to Phone B.
3. Phone B attempts to send video with the w360p resolution because there is no imageattr line in the SDP portion of the SIP header.

The following video call flow is between two 9951 phones (Phone A and Phone B) with imageattr line support (for example, using Cisco Unified Communications Manager releases 8.5(1) and later):

1. Phone A sends a SIP message with the imageattr line in the SDP.
2. Cisco Unified Communications Manager does not delete the imageattr line and sends the SIP message to Phone B unchanged.
3. Phone B attempts to send video with the VGA resolution.

CSCub12922 Adding a new subscriber causes device reset

When you add a new node to an existing cluster, all phones that are registered to the cluster are reset.

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 6 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.

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.

CSCtn32528 MLPP feature support only for SCCP phones

Only SCCP phones support the Multilevel Precedence and Preemption (MLPP) feature. SIP phones do not support MLPP. See the details in CSCtn32528.

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

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

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

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

There are 2 ways to resolve this issue:

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

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

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

Unrestricted Release Limitations

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

New in User Options Page Beta

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

Features Covered in the User Options Page Beta:

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

How to access the User Option Page Beta

The User Option Page Beta can be accessed at:

https://[UCM_HOSTNAME]:8443/ucmuser

The classic User Option Pages can still be accessed at:

https://[UCM_HOSTNAME]:8443/cucmuser

Limitations and Caveats with User Option Page Beta

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

CSCtq56727 SIP Gateway Crash During Heavy Call Traffic

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

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

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

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

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

CSCtq47285 RingOut State Transfer or Hold

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

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

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

utils diagnose module raid

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

```
show hardware
```

CSCtq46578 iso file download error message

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

- The first, which technically occurs before the file is downloaded, is to confirm that the file name of the file matches expected heuristics and rules of the upgrade. This heuristic and upgrade rules check can be executed remotely.

- A cryptographic digest of the downloaded iso file contents is then created and presented to the user in order to confirm the file's accuracy according to the Cisco web site. This process analyzes the contents of the iso, not the iso file itself, therefore the iso file must be mounted in order for the user to access its contents. The cryptographic digest process must be run locally on the server. If the iso file is corrupted, the cryptographic digest flags the iso as unusable and the operating system displays the following error message:

Buffer I/O error on device loop0, logical block

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

CSCto31364 Cluster Fully Qualified Domain Name (CFQDN) Parameter

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

CSCto83868 firmware update error message

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

Firmware update failing from 11.0.1.-0024

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

CSCtd87058 BAT Impact

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

- Configuring a Phone Security Profile - Device Security Mode field. Default specifies Non Secure
- Cisco IOS Conference Bridge Configuration Settings - Device Security Mode field. Default specifies Not Selected.
- Configuring Voice Mail Port Wizard - Device Security Mode field. Default value specifies Not Selected.
- Configuring Voice Mail Port - Device Security Mode field. Default specifies Not Selected
- Configuring SIP Trunk Security Profile - Device Security Mode field. Default specifies Non Secure.
- Configuring a Minimum Security Level for Meet-Me Conferences - Minimum Security Level field. The default specifies Non Secure

Call Park Feature Limitations

The Call Park feature has the following known limitations:

- CSCsz18443 Cisco Unified IP Phone 8961, 9951, 9971 Registered to a Node may Use the Call Park Number Assigned to Another Node, page 39
- CSCsz31137 Parked Call Gets Reverted When the Parkee is on, page 39
- CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve, page 39
- CSCtb53159 Display Limitation in ConfList, page 40

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

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

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

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

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

CSCsz31137 Parked Call Gets Reverted When the Parkee is on

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

CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve

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

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

CSCtb53159 Display Limitation in ConfList

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

CSCth53322 Rebuild Server After You Use the Recovery Disk

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

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

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

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

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

Condition

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

Workaround

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

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

Procedure

To change the OS Watchdog configuration setting:

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

Caution Do not configure any other timeout duration.

CSCtd01766 Destination Port on Trunk Remains Unchanged After Upgrade

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

CSCtl23382 Recovery CD Issues

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

When you boot the server from the Recovery Disk, the options that are summarized in Table 4 display:

Table 4 Recovery Disk Menu Options

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

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

To use the Recovery Disk, perform the following procedure:

Procedure

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

Step 2 Select the appropriate option from Table 4 on page 41.

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

Disaster Recovery System Caution

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

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

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

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

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

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

CSCtl47624 No Music On Hold when using ASR 1000

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

CSCtq20098 To handle DRS Restore status monitoring in a scenario

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

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

Procedure

Step 1 Conduct DRS Backup.

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

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

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

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

Limitations with Presentation Sharing when using a Cisco TelePresence MCU

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

Video Conferencing with Cisco Integrated Services Routers Generation 2

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

- Cisco 2900 Series
- Cisco 3900 Series

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

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

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

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

Interoperability with a Cisco TelePresence Video Communications Server

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

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

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

- VCS Interoperability Issues for Upgrades to Release 8.6.1, page 44
- Configuring VCS Interoperability in Release 8.6.1, page 44

VCS Interoperability Issues for Upgrades to Release 8.6.1

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

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

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

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

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

a. Click on the script to open the SIP Normalization Script Configuration window.

a. In the Name field, rename the script to anything other than *vcs-interop*. Cisco recommends adding the old release number to the script.

b. Click Reset.

Step 4 Proceed with the upgrade.

After upgrading to 8.6.1, complete Configuring VCS Interoperability in Release 8.6.1, page 44 to configure VCS interoperability in Release 8.6.1.

Configuring VCS Interoperability in Release 8.6.1

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

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

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

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

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

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

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

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

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

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

CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value

When you configure the MLPP Domain Name in Cisco Unified Communications Manager, the default name for MLPP Domain Name displays the MLPP ID value 000000 instead of Default as stated on the help page.

CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters

When configuring the Incoming Calling Party Numbers setting, the number of characters you can enter is 16 not 8 for:

- Incoming Calling Party National Number Prefix
- Incoming Calling Party International Number Prefix
- Incoming Calling Party Unknown Number Prefix
- Incoming Calling Party Subscriber Number Prefix

You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).

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 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.

CSCtr89029 URL Parameters for Secured Phones Repopulated After Restart

When you delete the Secured Phone URL Parameters in the Enterprise Parameter section of Cisco Unified Communications Manager Administrationand then reboot, the URL Parameters are re-populated by default. After you reboot go to the Secured Phone URL Parameters section and make the correct modifications to the URL and reboot the phones.

CSCtr62446 Route List Run on All Nodes Service Parameter

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

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.

CSCtr84167 Block Offnet to Offnet Transfer

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.

CSCtr21486 Troubleshooting Guide Update to Switch Version

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.

CSCtg67435 Certificate Regeneration During Domain Name Change

Using the set network domain CLI command to change the domain name triggers an automatic regeneration of all Cisco Unified Communications Manager certificates, including any third party signed certificates that have been uploaded. After the server reboots automatically, phones running in secure (mixed) mode cannot connect to the server until after the CTL client updates the new CTL file to the phones.

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 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.

CSCtw25693 MoH Does Not Support DTMF

Music on Hold (MoH) servers do not use or negotiate DTMF.

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.

CSCte43366 Japanese characters displayed as "_" in Music On Hold File

Japanese characters are displayed as "_" when you upload a wav. file as a Music On Hold File.

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.

CSCty75069 Secured Directory URL Enterprise Parameter overrides Directory field in Phone Configuration

If you configure a Secured Directory URL Enterprise Parameter in the Enterprise Parameters Configuration window, that value overrides the value in the Directory field in the External Data Locations Information section of the Phone Configuration window.

CSCtr44481 Download Dial Plans for Cisco Unified Communications Manager Release 8.X

You can download dial plans for Cisco Unified Communications Manager Release 8.X from the Downloads section of www.cisco.com. On the Cisco website, you can find the Cisco Option Package (COP) file that contains all the available dial plans that you can download, install, and integrate with Cisco Unified Communications Manager. For release 8.x, use the IDP v.3 cop files.

CSCty16160 During publisher node restores DB replication status must be 2 before you reboot the cluster

If you are restoring just the publisher node, before you restart the server, check the Replication Status value on all nodes by using the utils dbreplication status CLI command as described in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions. The value on each node should equal 2 before you restart the cluster.

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 Unifed Communications Solutions.

CSCtz83810 Directed Call Park MoH Audio Source Selection

If you are configuring directed call park music on hold, you must use the CallManager service parameter Default Network Hold MOH Audio Source in order to specify the audio source..

CSCtz73477 Interactions with Call Forward iDivert and Voice-Messaging features

The iDivert feature does not work in cases where the feature is initiated via CTI and the redirect signal must traverse a QSIG link.

CSCtq03342 Loading of selload: SELinux process takes up 100% CPU on CUCM

The Loading of selload: SELinux process takes up 100 per cent of CPU on Unified CM during boot up time. This will cause VMs to raise "High CPU alarms". The CPU stays at 100 per cent for about five minutes.

CSCtx86664 Port 6970 is open for HTTP requests to the TFTP server

Cisco Unified Communications Manager port 6970 is open for use by phones, which can make http requests to the TFTP server for new firmware.

CSCtu52978 Hard disk replacement fails if write cache is enabled on Cisco MCS 7828/28-i3

If you want to replace a failed RAID disk on a Cisco MCS 7825/28-i3 server and write-cache is enabled on the server, you must use the Disaster Recovery System to perform a backup before you perform this procedure. After you swap the hard drive, you must rebuild the server using the backup.

CSCtw79487 Default Device Pool may not be chosen after upgrades to 5.x or later

If you upgrade an existing system to 5.x or later and your system includes new device types, the Default Device Pool may not be selected for the new device types. After the upgrade, you must check to ensure that the Device Pool that you want is assigned.

CSCua75983 Support for midcall mobility features with Cisco Unified Border Element

Cisco Unified Mobility supports the Mobile Connect feature without mid-call features over SIP trunks with Cisco Unified Border Element (CUBE). To enable mid-call features, you must also configure an Enterprise Feature Access directory number and check the Send send-receive SDP in mid-call INVITE check box for the SIP profile that is assigned to the SIP trunk.

Failover/failback for dual mode phones

Failover and failback is supported for dual mode SIP phones. To support this feature, Unified CM node priority configuration on a dual mode handset should match the priority in the device pool on the Unified CM administration page. If a dual mode phone sends REGISTER to a lower priority CUCM node when the high priority node in its device pool is alive, it may generate a routing problem. The vendor must maintain the priority on nodes and synchronize them with Unified CM.

When a dual mode phone sends REGISTER to Unified CM, it may receive a 503 with a Retry-After header. This contains a time value indicating that Unified CM is not ready to accept registration.It expects the dual mode phone to re-attempt registration on the same node, after the specified time value is passed.

CSCth80282 Update regenerate certificate in Unified CM Operating System Guide

Certificate regeneration or upload of a third party signed certificate should be performed during maintenance.

If intracluster communication is enabled using EMCC complete the following steps during certificate regeneration.

Procedure

Step 1 Navigate to **Advanced Features > EMCC> Intercluster Service Profile** and deactivate **EMCC Service**.

Step 2 Logout all remotely logged in devices from **Device > Related Link > Remotely Logged In Device**.

Step 3 Regenerate certificates.

Step 4 Perform the Bulk Certification operation.

Activate the **EMCC Service**.

Secure shell password maximum length

The maximum length for a secure shell password is 50 characters. It can include any alphanumeric or special characters.

Only SIP re-INVITE is used for outbound transfers

Unified CM does not support SIP REFER outbound on SIP Trunks. It will support re-INVITE for outbound transfers.

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.

CSCub12688 FinalCalledPartyNumber CDR field description

The Cisco Unified Communications Manager Call Detail Records Administration Guide states that the FinalCalledPartyNumber record represents a numeric string of up to 48 characters that can be either digits or a SIP URL. This information is incorrect. The field can be greater than 48 characters and can be an alphanumeric string that can be either digits or a SIP URL.

CSCub17607 SIP Redirect by Application requires a SIP route pattern

If the Redirect by Application check box in the SIP Profile Configuration window is checked, and the option is configured on the SIP trunk, Cisco Unified Communications Manager passes the Contact header of the redirection request through its routing engine and applies routing logic to forward the redirection request to the address in the Contact header. If the host portion of the Contact header is not a local Unified CM, a SIP route pattern may be required to map the host portion of the Contact header to an outgoing trunk or Unified CM will not be able to route the call.

For detailed information on how Unified CM routes SIP requests, see "Routing of SIP Requests in Unified CM" in the Dial Plan chapter of the Cisco Unified Communications System SRND.

CSCub59376 Missing step in procedure for updating Unified CM hostname

There is a missing step in each of the procedures that describe how to change a server hostname in the Changing the IP Address and Hostname for Cisco Unified Communications Managers document. Immediately after you change the hostname of a Unified CM server and save your changes, the server automatically reboots. Immediately after the server reboots, you must bring up the Admin CLI for the server on which the hostname was changed and run the utils dbreplication dropadmin db command. This step applies to any procedure that involves a hostname change.

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.*

Tip 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.

CSCuc23992 Call Preservation support for SIP trunks

The Call Preservation feature in Cisco Unified Communications Manager also supports SIP trunks. Active calls that cross a SIP trunk do not get interrupted when a Cisco Unified Communications Manager node fails, or when communication between a device and its cluster node fails.

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".

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 54
- Restoring the First Node only (Rebuilding the Publisher Alone), page 57
- Restoring the Entire Cluster, page 59
- Restoring Subsequent Cluster Nodes (With or Without Rebuild), page 61

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 57. If you intend to rebuild the entire cluster, read the "Restoring the Entire Cluster" section on page 59.

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 57 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.

CSCug84842 Installation fails with unrecoverable internal error

When you install Cisco Unified Communications Manager, you must enter an Application User name and password. You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- Real Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User name - The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password - The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

Caution Do not use the system application name as the Application User name. Using a system application name will cause the installation to fail with an unrecoverable error during the installation of the database. System application names are:

CCMSysUser
WDSysUser
CCMQRTSysUser
IPMASysUser
WDSecureSysUser
CCMQRTSecureSysUser
IPMASecureSysUser
TabSyncSysUser
CUCService

You can change the Application User name and password by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

CSCun32117- Bulk Certificate Import May Cause Phones To Restart

The following note has been added to the Bulk certificate export section in the *Cisco Unified Communications Manager Security Guide* and the Configure EMCC section in the *Cisco Unified Communications Manager Features and Services Guide*.

Note When you use the Bulk Certificate Management tool to import certificates, it will cause an automatic restart of the phones on the cluster on which you imported the certificate.

CSCuo13148 Cisco ATA 187 Analog Telephone Adaptor Compatibility

The Cisco ATA 187 Analog Telephone Adaptor is compatible with Cisco Unified Communications Manager 8.0(3) and higher. For Cisco Unified Communications Manager 8.0(3), you must install the device pack cmterm-devicepack8.0.3.23038-1.cop.sgn for Cisco ATA 187 to be supported.

CSCuo10697 Updated List of LDAP Supported Directories

You can add users from your corporate directory to the Cisco Unified Communications Manager database by synchronizing the user data to the database. Cisco Unified Communications Manager allows synchronization from the following directories to the database:

Note This is an updated list for this release.

- Microsoft Active Directory 2003 R1 & R2 (32-bit)
- Microsoft Active Directory 2008 R1 (32-bit)
- Microsoft Active Directory Application Mode 2003 R1 & R2 (32-bit)
- Microsoft Lightweight Directory Services 2008 R1 (32-bit)
- Planet 5.1 & Sun ONE Directory Server 5.2
- Sun ONE Directory Server 6.x
- Sun Directory Services 7.0
- Oracle Directory Server Enterprise Edition 11gR1 (v11.1.1.5.0)
- OpenLDAP 2.3.39
- OpenLDAP 2.4

CSCup04321 Call Pickup Group Visual Notification does not Support Localization

The following limitation is applicable to Call Pickup:

Localization support is not available for call pickup group visual notification, as it uses ASCII for alerting name.

CSCtd43582 Remote Destination and Auto Answer

A remote destination call does not work when Auto Answer is enabled.

CSCup71020 MaxReturnedDevices in Serviceability XML

The Cisco Unified Communications Manager XML Developers Guide, Release 8.6 incorrectly specifies the maximum number of devices (MaxReturnedDevices) for which information can be returned in a search as 1000. The correct maximum number of devices is 200.

Outdated Information for Auto-Attendant

The Cisco Unified Communications Manager Auto-Attendant chapter contains outdated information around Cisco Customer Response Solutions 5.

For auto-attendant services, Cisco Unified Communications Manager can utilize compatible versions of Cisco Unified Contact Center Express. For details, refer to your Cisco Unified Contact Center Express documentation.

New and Changed Information

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

To obtain this document, go to the following URL:

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

Caveats

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

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

Resolved Caveats

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

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

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

Using Bug Toolkit

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

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

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

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

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

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

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

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

Open Caveats

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

Tip For more information about an individual defect, click the associated Identifier in the "Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011" section on page 67 to access the online record for that defect, including workarounds.

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

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

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

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

- 8.0(2.40000-x) = Cisco Unified Communications Manager 8.0(2c)
- 7.1(5.10000-x) = Cisco Unified Communications Manager 7.1(5)
- 7.1(3.30000-x) = Cisco Unified Communications Manager 7.1(3b)
- 7.1(3.20000-x) = Cisco Unified Communications Manager 7.1(3a)
- 7.1(3.10000-x) = Cisco Unified Communications Manager 7.1(3)
- 7.1(2.30000-x) = Cisco Unified Communications Manager 7.1(2b)
- 7.1(2.20000-x) = Cisco Unified Communications Manager 7.1(2a)
- 7.1(2.10000-x) = Cisco Unified Communications Manager 7.1(2)

Note Because defect status continually changes, be aware that the "Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011" section on page 67 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 66.

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

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

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

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011

IDENTIFIER	COMPONENT	HEADLINE
CSCts05068	sa-callp	CUCMBe3: Unable to make emergency call from Remote site post upgrade
CSCtj95738	database-ids	PMR 81654 database out of memory while syncing certificate table

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto77709	cpi-appinstall	Communication to Publisher lost after upgrade was started
CSCto81679	cp-mediacontrol	DTMF not working when MGCP gateway
CSCto84611	cp-supplementaryservices	CCM cores when running External Call Control automation
CSCto75049	cp-sip-station	Device Hold Reversion QED Settings Not Properly Checked
CSCtn97718	tftp	slave tftp server become unresponsive intermittently.
CSCto98215	cp-mediacontrol	MCNTRL-1054:RT-7985-ex90 transfer scenario [RT jitter]
CSCtl04228	cp-mediacontrol	Transfer fails - Unified CM 8 > 8.5.1
CSCtq04681	ccm-serviceability	SCH: Pub and Sub both becomes active during fallback
CSCtq10159	cp-mediacontrol	Unified CM tears down call if second TCS message is received in quick succession
CSCto68768	cmcti	Cannot control device after Migrate Phone until CTIManager restart
CSCtc87894	cp-mediacontrol	Video: UCM sends sendRecv instead of recvOnly for video call over ICT
CSCto17218	cpi-platform-api	Unable to locate files if folder contains names with special characters
CSCte05285	cpi-os	IBM I3 servers Automatic Server Restart (ASR) not enabled by default
CSCtf37698	cmcti	Incorrect reason code in ExistingCallEvent for supervisor
CSCto70998	cp-mediacontrol	Inter-cluster video call between LS & TB establishes as audio call.
CSCtg79013	security	tvs core when Pub/Sub1 switch back to old load after Sub2 install on new
CSCto71473	cp-mediacontrol	meetMee_wrong_reservation-410
CSCto71704	cp-mediacontrol	call_cannot-be_answered
CSCto71830	cp-sip-station	DeviceApplyConfigResult alarm definition is missing information
CSCth58139	cp-mediacontrol	sRTP:E2E-No Audio after simultaneous resume
CSCtl56249	c pi-os	User Prompt<Abort> on RU with less than minimum of disk on legacy models
CSCtn08912	database-ids	PMR 86128 corrupt syscdr resulting in bogus error 62 and/or 92
CSCtl56932	cpi-os	CORE cimserver on Sub while Pub is in process of Refresh Upgrade

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto76495	cp-mediacontrol	TRP wrongly handles DSCP markings for Video calls
CSCto77083	car	Hunt Pilot CFNA and CFB reports are not displaying in CAR
CSCto77125	car	Mismatch of Summary/Detail reports for hunt pilot failed and abandoned calls
CSCti69234	cpi-third-party	Security Issue in OpenSSL
CSCto80322	database-ids	Informix assert fail while running 3-day out of memory stress test
CSCto34641	cp-sip-trunk	Need a method to terminate/re-establish KPML subscription
CSCto68227	cmui	Configure Unassociated SD or BLF SD on Cius phone
CSCtn66109	cmcti	Get intermittent fail with Platform exception on transfer to another HP
CSCto86072	syslog	Cannot configure remote syslog on a subscriber node
CSCto87483	cp-mediacontrol	Get extra StartReception event after answer from redirect over sip trunk
CSCto88439	cp-mediacontrol	MCNTRL-1524:Bug in Agena Interface triggers unnecessary DTMF pro changes
CSCto88449	cp-mediacontrol	MCNTRL1532:MTPAgenaIF sends MXOffer before MXOffer recvd from SIF50
CSCto91596	cp-sip-trunk	DT: X-cisco-user-agent and server header sent incorrectly in xfer case
CSCto49535	cp-supplementaryservices	Call is not cleared from the line on phones by race condition of Pickup
CSCtn71568	cpi-os	Console login sometime doesnt works on Sub
CSCto94478	ims	No warning message when enabling SSO w/o importing OpenAM server cert
CSCtl74581	tapisdk	Mediariver w/ SRTP does not work on 64Bit client
CSCto02728	cmui	Unified CM web very slow for phone queries
CSCto95129	tapisdk	no CONFERENCED call state (IDLE) on Target in app on cBarge
CSCto51280	cp-callcontrol	Two G729 calls consume 160kbp of location bandwidth
CSCto51306	cmui	Slow Admin on Device Search by Device Pool
CSCtk32432	cpi-third-party	Update TPL OpenSSL to Addresss Published Vulnerabilities
CSCto96586	cp-sip-trunk	No audio after blind transfer when SIP SP does not support UPDATE

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto96924	cp-mediacontrol	E2E hold-resume video call results in audio call for resumed connection
CSCto72113	cpi-appinstall	uc86-gb-sol
CSCto99391	ccm-serviceability	SCH: Passed-time messages are not sent in the fail over scenarios
CSCto57127	cp-mediacontrol	e2e: hairpin call between EX-90 & RT phone has no video
CSCto57427	cpi-os	Cannot ping ipv6 addresses outside its own subnet from 8.6 Unified CM
CSCtq00323	ccm-serviceability	SNMP agent needs to filter processnodeservice CNs
CSCtn50334	cpi-appinstall	Applying refresh_upgrade COP file after canceled RU gives wrong prompt
CSCto57934	cp-mediacontrol	DTMF sent by the caller does not reach the callee.
CSCtg93134	ccm-serviceability	utils system restart cli command gives error
CSCti81686	cp-mediacontrol	CUBE Does not update the Media Info from ACK/SDP followed by PRACK/SDP
CSCtn00989	cmui	CCMAdmin shows registration unknown after Android registered
CSCtq01514	cp-sip-trunk	Additional Characters in SDI logs when a call made via QSIG SIP Trunk
CSCtq01756	cpi-os	Update NSS RPMs per RHSA-2011:0472-1
CSCto09866	cmcti	Unable to create conference chain with conference bridge
CSCtq04067	cp-sip-station	“Unknown Number” is displayed when "Auto Pickup" is enabled
CSCtq05761	cp-mediacontrol	Blind conferencing over H.323 and SIP EO fails
CSCtn82607	database	PMR 89829 CCM 8.6.0.96071-5: Error 403 during cdr check w/ verbose
CSCtn90839	cuc-tomcat	Adjust Tomcat memory diagnostic to take into account free memory
CSCtq06789	cp-sip-station	“findDeviceByX509Subject: No Entry Found” lines filling the Unified CM traces
CSCtn84005	cp-mediacontrol	h245 session gets stuck after sending the ECS
CSCto62290	cp-sip-station	ApplyConfig does not work when SIP Profile is changed on vsrious RT phones.
CSCto62450	cp-mediacontrol	Attended Xfer of conference over H.323 trunk fails
CSCtq07868	cp-mediacontrol	No MOH for sRTP MGCP FXS endpoint when placed on hold
CSCto11698	database-ids	PMR 00006 data is not replicating between all nodes in cluster some
CSCtq07935	sw-phone-sip	Blind beginEndTransfer failed (phone 2 “ringout” was not cleared)

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq08137	sdl	outgoing connections network trace can crash application
CSCtl44984	database-ids	PMR 84728 Assert Failure yield_processor: Conditional latch count non-ze
CSCtl44987	database-ids	PMR 84726 Assert Failure Fatal Error In Buffer Manager
CSCtq09875	axl	Get License Capabilities failed with UserID having Apostrophe
CSCto17792	cpi-appinstall	Cisco Unity Connection error code ignored by platform during refresh upgrade
CSCtq10460	jtapisdk	Fail to get hunt connection when tranfer to another hunt pilot
CSCtn86264	cpi-os	IBM cimlistener process crashed unexpectedly
CSCtl88901	cpi-os	usb_key_detect core during RU from 6.1.5.10000-7 to 8.6.0.94000-88
CSCto52689	axl	Language not localized in directory page
CSCto71448	cpi-service-mgr	After CUCM upgrade few services operational status remains down
CSCto82031	cmui	Login error message provides too much information
CSCtq19020	database-ids	PMR 04791 Assert duriXng out of memory testing on 55GB virtual server
CSCtq72623	cp-system	Code yellow under mobile agent NailUp load
CSCtq14129	cp-system	CCM Cored After upgrade to 8.5.1.12018-1
CSCtq70875	backup-restore	CUCM,CUCMBE3000 8.6 - Manual backup job cancellation doesnt terminate.
CSCtq74604	ime-server	IME - Calls to a site who disables IME often fail
CSCtq75780	cp-huntlist	RouteList control not returning - CcRejInd back to correct Cdcc
CSCtq37605	cp-sccp	Lines could not register after SdlLinkOOS
CSCtq41333	cp-sccp	Route list prefix shows up at the caller phone
CSCtq75566	ims	Single Sign On cant be enabled on Unity Connection
CSCtq70900	cpi-cert-mgmt	Tomcat and/or IPSEC Key store corruption causes DRF backup failures
CSCtq55418	cp-mlpp	Receiving Phone always gets Routine MLPP instead of Priority, Flash etc
CSCtq63440	smdiservice	Error reported on console during bootup for usbserial and pl2303 modules
CSCtq67098	cp-digit-analysis	CUCM crashes when LD number is dialed for Germany country pack
CSCtq36661	ext-mobility	HEB: Extension Mobility Menu show up in English for Hebrew Locale

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq37634	cp-device-manager	Lines could not register after SdlLinkOOS
CSCtq40657	cp-qsig	Issue with QSIG over SIP. MWI relay to ISDN PRI QSIG trunk failing
CSCtq22979	rtmt	RTMT login issue when Cisco DB is down
CSCtq76930	risdc	8.6.1.96000-11 mo_main (VIPR) Build Status Is FAILED
CSCtq76428	cp-sip-station	UCM cores when sip station parses corrupt XML in SIPNotifyInd signal
CSCtq43535	cp-sip-trunk	"c=" SDP line not included in media level BFCP line in certain cases
CSCtq46039	cp-sip-trunk	Renegotiation SDP syntax incorrect for ANAT call
CSCtq47472	cp-sip-trunk	CUCM Codeyellow/Coredump due to SIP ICT connectivity lost.
CSCtq52484	cp-sip-trunk	4_parties_exit_conference_end_other-2-drop-call
CSCtq59044	cp-sip-station	softphone conference not working properly
CSCto58617	cp-sip-station	Servitude: Incoming call not working after 2 x blind transfers
CSCto66595	cp-sip-station	Cius re registers when an app is subscribed from CUCM
CSCtq00065	cp-sip-station	Speed dial w/ 9 prefix does not dial out
CSCtj87367	cp-sip-trunk	Code Yellow / Core Dump after upgrade
CSCtq57368	cp-sip-trunk	SIP Polycom doesnt negotiate video via h.323 trunkm
CSCtq67392	cp-sip-trunk	Transfer from CUCIMOC to E20 via h.323 trunk fails
CSCtn79239	cp-sip-trunk	CTS to VC call via a CUCM hop fails
CSCtq15868	cpi-appinstall	password from pwrecovery sometime no work after RU to new load
CSCtq52311	cpi-appinstall	install_log_migrate script failed to tar log files cause L2 upgrade fail
CSCtq66557	cpi-appinstall	L2 upgrade to 9.0 and above fails.
CSCtq68899	cpi-appinstall	Upgrade process needs to cleanup refresh upgrade files
CSCtq74591	ime-appinstall	IME Refresh upgrade on 7825H3 failed
CSCtq62914	ime-csa	After Switchback with IME to 8.51. from 8.6.1, wrong inactive version
CSCtq30093	cuc-tomcat	DT: Tomcat cores when using utils system restart
CSCtq38115	cpi-platform-api	getClusterNodes platform SOAP service only returns 1 node
CSCtq69347	cpi-os	IPv6 address not restore from backup
CSCtq71010	bps-bat	RU upgrade fails due to bps migration script failing

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq71338	qed	Create New Product CSV file for AS Third Party SIP endpoint
CSCtq56857	dial-num-analyser	DNA not analyzing routes correctly - SQL error
CSCto43487	ccmcip	HEB: 8945: Hebrew personal directory service show up in English
CSCtg79013	security	tvs core when Pub/Sub1 switch back to old load after Sub2 install on new
CSCtq52222	selinux	Stopping auditd and setroubleshootd failures displayed during U1 boot up
CSCtq53442	cpi-os	7890C1 USB key present during re-image forces user interaction
CSCtq72631	security	TFTP Certificate in system file out of sync with database
CSCtq24472	cp-mediacontrol	No video after xfer : Allow2833 variable set incorrect
CSCtq73405	cp-mediacontrol	1-way video on SCCP Gumbo after TimeoutWaitingForVideoOLCAck
CSCtq73524	cp-mediacontrol	1 way video with SCCP Gumbo to RT over DO SIP trunk
CSCtq74688	cp-mediacontrol	CTS 500 call gets dropped after the originator of the conference is rele
CSCtq76667	cmcti	CTIManager memory leak due to LDAP/SSL failures
CSCtq41065	cmcti	No ConnectedID with cbn number on DTAL after conference chain
CSCtq43478	cmcti	Incorrect partition is reported in CPIC after start whisper coaching
CSCtq73859	cp-supplementaryservices	Agent Greeting Call failure during load test
CSCto80476	jtapisdk	CallCtlConnDisconnectedEv received after TransferEnd
CSCtq55887	cp-mobility	CUCM phone and had RD pickup. Remote In Use is not there for Desktop
CSCtq71085	cp-mobility	Intelligent Session Control CFNA to VM uses cell as fwding DN
CSCtq18031	cp-mediacontrol	Failed media resource (MTP) allocation leads to CCM core
CSCto00448	cmui	Unable to access menus on CCM User page from native browser on CIUS
CSCto59013	cp-mediacontrol	No Video when CTS to EX90 call over H323 is hold/resume from CTS.
CSCtq13000	cp-sip-station	CM Coredump under traffic load.
CSCtq47636	cp-sccp	CUCM core on MB 8.6.1.10000-26

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq43709	cpi-appinstall	L2 Upgrade Failure install_rpms
CSCto63870	cp-sip-station	503 Service unavailable in station_close state after SIP line reset
CSCtq42857	media_str_app	UCCX Intermittent Kernel Panic when Media --> Recording Step is Accessed
CSCtq41895	sa-maintenance	IE9: HTTP 404 status page on initiating Upgrade COP File in Morpheus
CSCtq35070	axl	AXLThrottler causing high Tomcat CPU
CSCtq22061	cp-mediacontrol	Can't resume SIPT call between Tandbergs with region pair at 32kbps
CSCto85294	cp-mobility	Mobility softkey / button stops working after failed hand-in
CSCto73185	vapi-real	RT Lite automation fails on makeCall
CSCto73005	cp-mgcp	CUCM responds with non user value to Status Enquiry
CSCto73285	webdialer-service	Webdialer - CTI service unavailable message not displayed
CSCsr00340	cmui	Dependency records should show ExtensionMobilityDynamic records
CSCto74049	car	Summary report is calculating wrong data in Manager/Assistant report
CSCto80767	axl	Products assigned to users in CUCM are not showing up in CUPM
CSCto81448	cp-sip-trunk	Get no audio for mid-call transfer over SIP ANAT with MTP ICT
CSCto81820	cmui	Device profile disappears after saved in the app user CTI control Device
CSCto83868	cpi-os	7835/45-I3 fresh install has Raid firmware update failure
CSCto86462	cp-mobility	Mobility layer should send RelInd When DisconnReq contain Invalid CI
CSCto89349	cp-sip-station	Incorrect Fid used during Chaperone conference created with CallJoinReq
CSCto91102	bps-import-export	Validation for featurecontrolpolicy.csv failed in Export/Import Tool
CSCto91859	cp-sip-trunk	Hold on phone with SIPT--H.323 ICT hairpin transfer call will drop the c
CSCto94339	cp-sccp	Incorrect Fid used during Chaperone conference created with CallJoinReq
CSCto96231	axl	Can't assign the Moblity user ID using addPhone request
CSCtg41133	inter-dial-plan	Check-in of Text and Csv files for India,China into Clearcase

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto96586	cp-sip-trunk	No audio after blind transfer when SIP SP does not support UPDATE
CSCto98070	voice-sipstack	CUCM ignores subscribe refresh from TB endpoint
CSCto99256	cpi-os	CLI hangs with invalid login while enabling kdump for external SSHserver
CSCti60031	cp-sip-trunk	Re-order tone in originating side(CUCM) for unanswered CME call
CSCto99699	ccm-serviceability	Syntax error in naaagt script affects the naaagt's consistant performanc
CSCtj20695	rtmt	Alarm Definition Help not coming for Alarms with SubFacility having "_"
CSCtq06339	bps-import-export	Import of entities with no records showing error
CSCtj51295	cp-mediacontrol	CTS issue with CUCM reinvite with H.323 endpoints
CSCtj52266	tftp	MLPP domainId, MLPPIndication Status, Preemption from phone config page
CSCtq07325	sa-mac	While configuring translation rules, rules vanishes randomly
CSCtq09875	axl	Get License Capabilities failed with UserID having Apostrophe
CSCtk11498	cmcti	Wrong Join/DT/JAL/DTAL info with default setting on 69xx/89xx-SIP
CSCtq11687	axl	UpdateUserGroup failed with UserID having Apostrophe
CSCtq11834	axl	UpdateLicenseCapabilities failed with UserID having Apostrophe
CSCtk65829	cp-mediacontrol	Call transferred to video device does not result in audio call overflow
CSCtq13534	cpi-os	"Error 15: File not found" shown in install log for install 8.6.1 on top
CSCtq13947	cpi-os	Update Python per RHSA-2011:0491-01 and RHSA-2011:0492-1
CSCtl43943	dial-num-analyser	DNA does not show local route group information
CSCtq15955	voice-sipstack	fix the SIP Stack SA warinng in MB 5-5-2011 report
CSCtq17311	media_str_app	Software MTP does not change payload type for RFC2833 DTMF
CSCtq18720	bps-bat	Bulk Administration file/log migration of RU from 7.1.5 to 8.6.1
CSCtl74266	cpi-afg	CUCM should validate X.500 O, OU string length in Answer File Generator
CSCtq20483	cp-sip-station	ATA 187fails for "Speed Dial Await Further Digits", if set to true

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq24941	database	Fix SA warnings in cc_mainline for DBL2 MontBlanch issues
CSCtq27136	cp-sip-trunk	Refixing CSCti60031 - Re-order tone in originating side(CUCM) for unansw
CSCtq27720	cp-sip-station	connected number of the call back call is unknown
CSCtq28446	cp-bri	MontBlanc Static Analysis Issues related to MGCP Source files
CSCtq34932	cp-mgcp	DCP call hears ringback instead of MOH when MGCP is involved.
CSCtq35910	cpi-os	Cancel during install wizard detects existing good format as wrong one
CSCtn39639	cp-sip-station	CUCM incorrectly subscribes for KPML during CFW activation
CSCtq37461	cmui	CCMAdmin does not load properly on IE
CSCtq37975	cmcti	CTI manager using "NULL" devicePkid, causing CAD login issues
CSCtn51784	rtmt	Incorrect Error Message while launching RTMT
CSCtq38115	cpi-platform-api	getClusterNodes platform SOAP service only returns 1 node
CSCtq38433	cp-sip-trunk	S1/S2 Static Analysis error in sip-trunk and sip-line components
CSCtq40041	axl	Add Remote Destination Profile get failed with UserID having Apostrophe
CSCtq40768	tapisdk	LineGetCallInfo exception
CSCtq42131	sa-maintenance	Valid MD5 Checksum Validation Fails in Morpheus build
CSCtq43347	ccm-serviceability	L2 Upgrade Fails Due to CCM Service Not Registered in DB Correctly
CSCtq43523	cmui	Roaming Settings not shown in UI with high number of CSS or Device Pools
CSCtq43975	cp-sip-trunk	Calls in alpha failing due to issues with Early Media Cut-Through
CSCtn86627	bat	BAT:Assign 30K users to SC's failed, memory issue and Jabbard core
CSCtn87207	cp-mediacontrol	Two G729 calls consume 160kbp of location bandwidth
CSCtq44339	cp-sip-trunk	SIP layer sends out multiple codecs in the Offer when MTP required is ch
CSCtn97852	cpi-appinstall	"cimsubscribe" CORE due to RU server_specific_install.sh issue
CSCtq49089	axl	Remove Subscriber get failed with UserID having Apostrophe

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCtq50205	cmui	ucmuser-beta contextlistener for locale
CSCtq51390	cp-pri	Incoming redirecting IE is discarded if digits are preficed with +
CSCtn99418	ccm-serviceability	CarIDSPerfmon Job Fail Alerts in Logged in Syslog File
CSCto01403	bps-import-export	Job status error during import in bulk admin tool
CSCtq54940	media_str_app	DTMF over RFC2833 fails as S/W MTP doesnt set correct seq number or SSRC
CSCtq55224	cmui	Phone configuration page takes long time to load
CSCtq57173	axl	Unable to perform Change Order for the attribute : Calling Search Space
CSCtq59447	bps-import-export	Import with override fails for CTIRoutePoint
CSCto07944	webdialer-service	Problem in interaction between Webdialer and EM service
CSCto11430	cp-rsvp-agent	Race condition leading to Contact Center Calls Get Stuck in Queue
CSCtq63408	cp-mediacontrol	Renegotiation during MeetMe with MTP has wrong profile level.
CSCtq65343	vapi-real	complete and commit changes to merlin for gumbo sccp support
CSCtq69347	cpi-os	IPv6 address not restore from backup
CSCto25077	cp-sip-station	Sip phone hears ringback tone when calling busy line on PRI
CSCtq79105	voice-sipstack	Fix handling of dbl incremented cseq
CSCto36517	bps-import-export	Users Associated with Line is not exported by BAT
CSCto43412	cp-supplementaryservices	Hunt Call hang when conferneced call go back to 2 party call
CSCto45744	cp-mediacontrol	EX90 to EX90 E2E RSVP call failing when region pair max audio is 32 kbps
CSCto45772	cp-mediacontrol	H323-SIPICT-E20 hold/resume from E20 doesn't work for Audio G7221 codec
CSCto45800	cp-mobility	MGCP EFA call got busy tone with Dragon login
CSCto46211	tapisdk	no CONFERENCED call state on Target in app on cBarge
CSCto50580	cp-sip-trunk	One way video on RT with call flow RT-VCS/C20--need updated Lua script
CSCto50730	cp-mobility	Dragon DVO transfer/add call doesnt work
CSCto51150	database	setrepltimeout command does not indicate success/failure of command
CSCto52071	cpi-os	dhcpd req's manual restart if NFT enabled/disabled
CSCto53232	voice-sipstack	CUCM ignores subscribe refresh from TB endpoint

Table 5 Open Caveats for Unified CM Release 8.6(1a) as of June 24, 2011 (continued)

CSCto54048	cmcti	CTI Manager not reporting the correct device handle
CSCto56209	cp-sip-trunk	CUCM includes diversion header when doing called party transformation
CSCto58469	cp-sip-trunk	Secure/encrypted call to SIP Service Provider call disconnects after OK
CSCto58904	cp-mediacontrol	Floor control role incorrect in re-INVITE glare scenario
CSCto60019	cli	utils network ipv6 traceroute command does not work
CSCto60097	tapisdk	Dynamic tracing is not working if app opened Provider and lines
CSCto60189	cp-mobility	Android can't reg as VOIP when MI not config'd after trying reg as cell
CSCto62746	voice-sipstack	FECC does not function on MXP 1500 (H.323)
CSCto66019	cp-mobility	correct Cisco Dual Mode for Android product and model monikers
CSCto70180	cp-mediacontrol	Call between RT & TB drops on resuming the call on RT phone.
CSCto70998	cp-mediacontrol	Inter-cluster video call between LS & TB establishes as audio call.
CSCto71473	cp-mediacontrol	meetMee_wrong_reservation-410
CSCto72113	cpi-appinstall	Upgrade process tries to switch version even though upgrade does not com
CSCto72188	jtapisdk	Get NPE on conference with codian conference bridge

Documentation Updates

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

- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 79
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 79
- Directory Number Field Description Updated, page 80
- E & M Port Configuration Settings, page 81
- Cisco Unified Communications Manager Call Detail Records Administration Guide, page 81
- FAC and CMC Code is not Captured in CDR, page 84
- Cisco Unified Communications Manager Features and Services Guide, page 88
- Cisco Unified Communications Manager Administration Guide, page 89

- Cisco Unified Communications Manager TCP and UDP Port Usage, page 92
- Cisco Unified Serviceability Administration Guide, page 92
- Troubleshooting Guide for Cisco Unified Communications Manager, page 93
- Cisco Unified Communications Manager System Guide, page 95
- Cisco Unified Communications Manager Security Guide, page 95
- CSCus63274 Devices Reset After Certificate Regeneration, page 97
- Cisco Unified Real-Time Monitoring Tool Administration Guide, page 100
- Command Line Interface Reference Guide, page 101

Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service

- Domain Name Change for Cisco Unified Communications Manager, page 79

Domain Name Change for Cisco Unified Communications Manager

This documentation update resolves CSCuw76028.

The following information is omitted from the " Domain Name and Node Name Changes" chapter in the *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service Guide*.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications
Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

Before You Begin

- Perform all pre-change tasks and the applicable system health checks.
- Ensure to enable the DNS before changing the domain name.
- If the server table has an existing hostname entry, first change the hostname entry of the domain name.

Step 1 Log in to Command Line Interface.

Step 2 Enter **run set network domain <new_domain_name>**

Step 3 Click **Yes** to reboot the system.

Step 4 Enter the command **show network eth0** to check if the new domain name is updated after the reboot.

Step 5 Repeat this procedure for all cluster nodes.

What to Do Next

For more information, see the " Post-Change Tasks and Verification" chapter in the *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service guide*.

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, page 80
- Device Name and Description fields need to be updated, page 80
- Directory Number Field Description Updated, page 80

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 (<>).

Directory Number Field Description Updated

This documentation update resolves CSCuy28500.

The following note is omitted from the “Directory Number Settings” topic in the online help and “User Device

Profile Fields Descriptions in BAT Spreadsheet” topic in the *Cisco Unified Communications Manager Bulk Administration Guide*:

Note The “Disable ” or “Flash only” setting options apply only for the handset. The led light on the phone button line will still flash.

Clarification of Log Missed Calls Check Box

The description of the Log Missed Calls check box in the Directory Number Configuration chapter is implies that the Log Missed Calls check box applies only to shared lines. However, the Log Missed Calls check box applies to both shared phone lines and non-shared phone lines.

If the Log Missed Calls check box is checked, Cisco Unified Communications Manager logs missed calls in the call history on the phone. If the check box is unchecked, Cisco Unified Communications Manager does not log missed calls. The default setting for this check box is checked.

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 81
- CDR Field Descriptions, page 81
- Incorrect CDR Field Description for destCallTerminationOnBehalfOf, page 83
- FAC and CMC Code is not Captured in CDR, page 84

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 6 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 7 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	This field indicates the transmitting resolution. In the case of the H.264 codec or a 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.
destVideoCap_Resolution	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution	This field indicates the transmitting resolution. In the case of the H.264 codec or a 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.

Field	Range of Values	Description
origVideoCap_Resolution_Channel 2	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16 6 = H263 custom resolution	This field indicates the transmitting resolution for the second video channel. In the case of the H.264 codec or a 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.
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	This field indicates the transmitting resolution for the second video channel. In the case of the H.264 codec or a 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.

Redirect Reason Codes

Table 8 Redirect Reason Codes

Value	Description
178	Call Forward Unregistered

Incorrect CDR Field Description for destCallTerminationOnBehalfOf

The description for the destCallTerminationOnBehalfOf field erroneously states “For example, if the originator of the call hangs up the phone, the OnBehalfOf code shows ‘12’ for Device. If the call terminates because of a transfer, the OnBehalfOf code shows ‘10’ for Transfer.” The term “originator” should read “destination.”

Incorrect Order of CDR and CMR Fields

Some CDR and CMR fields are in the wrong order. See the following tables for the order in the document and the corrected order:

Table 9 CDR Fields Order Corrections

Order in Document	Corrected Order
callIdentifier	directoryNumber
directoryNumber	callIdentifier

Table 10 CMR Fields Order Corrections

Order in Document	Corrected Order
deviceName	globalCallId_ClusterId
globalCallId_ClusterId	deviceName

FAC and CMC Code is not Captured in CDR

This documentation update resolves CSCus91749.

The following information about CDR entry for FAC and CMC calls is omitted in the Forced

authorization code (FAC) and Client Matter Code (CMC) topic in the Cisco Unified Communications Manager Call Detail Records Administration Guide.

FAC

CDR will now be written for a setup call leg for all the unanswered calls before the call is redirected to another caller if FAC is used to setup the call.

Note This call will not have any connect time since media is not connected for this call. The CDR will be logged regardless of the service parameter **CdrLogCallsWithZeroDurationFlag** if FAC is present in the call.

FAC Example 2

Blind conference using FAC:

Step 1 Call from 136201 to 136111.

Step 2 136111 answers and speaks for a few seconds.

Step 3 136201 presses the **Conference** softkey and dials 136203.

Step 4 The user is prompted to enter the FAC code and the user enters 124. FAC code 124 is configured as level 1 and given a name as Forward_FAC.

Step 5 While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.

Step 6 136203 answers the call.

Step 7 The three members in the conference talk for sometime.

Step 8 136111 hangs up, leaving 136201 and 136203 in the conference. Since there are only two participants in

the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60015	60016	60015	60015	60015	60017
origLegCallIdentifier	23704372	23704374	23704373	23704372	23704376	23704377
destLegCallIdentifier	23704373	23704376	23704381	23704380	23704382	23704378
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_FAC				
authorizationLevel	0	1	0	0	0	0
Duration	18	0	37	37	32	38
authorization Code		124				

Note The setup call CDR for this example is generated even though it is of zero duration since FAC is used for this call.

CMC Example 2

Blind conference using CMC :

Step 1 Call from 136201 to 136111.

Step 2 136111 answers and speaks for a few seconds.

Step 3 136201 presses the **Conference** softkey and dials 136203.

Step 4 The user is prompted to enter the CMC code and the user enters 125. CMC code 125 is configured as level 1 and is given a name as Forward_CMC.

Step 5 While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.

Step 6 136203 answers the call.

Step 7 The three members in the conference talk for sometime.

Step 8 136111 hangs sup, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60025	60026	60025	60025	60025	60027
origLegCallIdentifier	23704522	23704524	23704523	23704522	23704526	23704527
destLegCallIdentifier	23704523	23704526	23704531	23704530	23704532	23704528
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_CMC				
authorizationLevel	0	1	0	0	0	0
Duration	20	0	32	32	25	48
authorizationCode		125				

Note The setup call CDR for this example is generated even though it is of zero duration since CMC is used for this call.

Disaster Recovery Administration Guide

The following changes exist for Disaster Recovery Administration Guide for Cisco Unified Communications Manager:

- Managing Backup Devices, page 87
- Running Backups or Restores, page 87

- Alternative SFTP Servers, page 87
- DNS Information During Restore, page 87
- Updated Caution to include DNS and Domain Name prior to restore, page 87

Managing Backup Devices

This update applies to *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager*. In Step 6 of the Managing Backup Devices section, it says that the backup device name may contain spaces. This is incorrect. The backup device name may contain alphanumeric characters, dashes (-), and underscores (_). Spaces are not allowed.

Running Backups or Restores

This update applies to backup and restore procedures in *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager*. When running backups or restoring backups on a Cisco Unified Communications Manager server, make sure that all nodes in the cluster are running the same version of Cisco Unified Communications Manager. If different nodes in the cluster are running different versions of Cisco Unified Communications Manager, you will end up with a certificate mismatch and your backup or restore could fail.

Alternative SFTP Servers

This update applies to the Disaster Recovery System Administration Guide for Cisco Unified Communications Manager. The System Requirements section contains out of date information about the Cisco Technology Developer Partner program (CTDP). This section should read as follows:

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco Technology Partners. Technology 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 Solutions Catalog on the Cisco Developer Network. The Solutions Catalog is accessible at:

https://marketplace.cisco.com/catalog/search

DNS Information During Restore

DNS is not mentioned in the *Disaster Recovery System Administration Guide*. The guide should state that the DNS Configuration on the server prior to restore should be the same as the DNS Configuration when the backup was taken.

Updated Caution to include DNS and Domain Name prior to restore

The following caution is updated to include DNS and domain name prior to performing a restore:

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

Cisco Unified Communications Manager Features and Services Guide

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

- Remote Cluster Menu Path is Incorrect, page 88
- DoCoMo Phones Not Certified, page 88
- Early Media Cut-Through and Single Number Reach, page 88
- Configuring OpenAM Section, page 88

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**.

DoCoMo Phones Not Certified

The Remote Destination Configuration Settings section that appears in the "Cisco Unified Mobility" chapter of the Cisco Unified Communications Manager Features and Services Guide states that the Mobile Phone check box does not apply to dual-mode phones that are running SIP, such as DoCoMo N902iL and DoCoMo N906i. This information is correct. However, the DoCoMo phones should not be explicitly mentioned since neither phone has been certified with Cisco Unified Communications Manager.

Early Media Cut-Through and Single Number Reach

The following information is missing from the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*:

Early Media cut-through is not supported for Single Number Reach (SNR) calls. SNR follows shared line behavior and does not function as desired with early media cut-through.

For example, Phone A (DN 1000) calls Phone B (DN 1001) which has an Remote Destination Phone C(DN 1001), sharing line with Phone B . When you enable early media cut-through and place a call to Phone B, both shared lines do not ring, because with early media cut-through enabled, a device may signal a connect, causing the other device to stop ringing.

To avoid this behavior, do not configure early media cut through on the outbound trunk or gateway for SNR.

Configuring OpenAM Section

The following content is missing from the "Configure OpenAM" section of "Single Sign-On" chapter:

After you install the OpenAM server, you must ensure that a default account is created so that you can enable and configure the SSO-based authentication successfully on Cisco Unified Communications Manager applications. The default account consists of a "demo" username and a password. To enable Agent Flow SSO on Unified Communications applications, the system uses this default account to validate the following that are provisioned on OpenAM:The following content is missing from the "Configure OpenAM" section of "Single Sign-On" chapter:

- Login module

- J2EE agent

To verify if the “demo” user is configured or not, perform the following procedure:

Procedure

Step 1 Log in to the **OpenAM** server.

The OpenAM administration window appears.

Step 2 Select the **Access Control** tab.

A list of one or more access control realms appears.

Step 3 Click **Top Level Realm**.

Note The top level realm appears in the list when you deploy the OpenAM server. This realm contains the OpenAM configuration data.

An additional set of configuration tabs appears.

Step 4 Select the **Subjects** tab.

Step 5 Click **New**.

A list of fields containing user details appears.

Step 6 Enter data for the following fields:

- **ID**: demo
- **First Name**: demo
- **Last Name**: demo
- **Full Name**: demo
- **Password**: changeit
- **Password (confirm)**: changeit

Note Do not change this default password.

- **User Status**: Select the **Active** radio button.

Step 7 Click **OK**.

The system creates a “demo” user successfully.

Cisco Unified Communications Manager Administration Guide

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

- Correction in Software Conference Bridge Maximum Audio Streams, page 90
- Correction in Software Conference Bridge Maximum Audio Streams, page 90
- Removed field Call Stats from SIP Profile configuration, page 90
- Relabel of Use Personal Preferences field, page 90

- CSCuh62299 Note added to the Service Name field, page 91
- Added description for For voice mail usage option in Add hunt list procedure, page 91
- CSCup45037 Transmit UTF8 for Calling Party Name Field Correction, page 91
- Incorrect Note about User Locales, page 91

Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu44805.

The maximum audio streams per software conference bridge is incorrectly listed as 128 in the

“Software Conference Devices” section of the Cisco Unified Communications Manager Administration Guide.The correct value is 256.

Updated field descriptions for Timer Register Delta and Timer Register Expires

Following are updated field descriptions for Timer Register Delta and Timer Register Expires:

Timer Register Delta

This field is intended to be used by SIP endpoints only. The endpoint receives this value via a tftp config file. The end point reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values for Timer Register Delta range from 32767 to 0. The default value is 5.

Timer Register Expires

This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value via a tftp config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value.

If the endpoint sends a shorter Expires value than the value of the SIP Station Keepalive Interval service parameter, Cisco Unified Communications Manager responds with a 423 "Interval Too Brief".

If the endpoint sends an Expires value that is greater than the SIP Station Keepalive Interval service parameter value, Cisco Unified Communications Manager responds with a 200 OK that includes the Keepalive Interval value for Expires.

Note For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.

Removed field Call Stats from SIP Profile configuration

In the “SIP profile settings” section, the field “Call Stats” is not available under **Device > Device Settings > SIP Profile** on the Cisco Unified Communications Administration page. The Call Stats field is enabled, by default.

Relabel of Use Personal Preferences field

In the **Call Routing > Route/Hunt > Hunt Pilot** setup window, the **Use Personal Preferences** option has been renamed to **Use Forward Settings of Line Group Member**.

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.

Added description for For voice mail usage option in Add hunt list procedure

The following description about For voice mail usage option has been added to the Add hunt list procedure in step 6:

"If you check the For Voice Mail Usage check box, the route list control process keeps a count of the setups that are being served to the hunt list, and will not allow more setups than the number of available devices. As a result, each device in the hunt list is treated as if it has a Busy Trigger and related Maximum Number of Calls of one".

"For example, if the hunt list contains five devices, and if busy trigger is two for each member, with the For Voice Mail Usage checkbox unchecked, it can process up to ten setups. For the same number of hunt list devices with a busy trigger of two for each member, with the For Voice Mail Usage checkbox checked, it can process only five setups and the next immediate setup after five gets rejected".

CSCup45037 Transmit UTF8 for Calling Party Name Field Correction

The *Cisco Unified Communications Manager Administration Guide* specifies that the SIP-trunk field Transmit UTF-8 for Calling Party Name is defined as using the user locale setting of the device pool in determining what to send in the Calling Party Name field. However, the device pool does not have a user locale field, it has a network locale field, and both the Common Device Configuration record and the Phone record itself have user locale fields.

The following is the process that the SIP trunk uses to obtain the user locale:

If the Transmit UTF-8 for Calling Party Name is checked to obtain the locale, the SIP trunk attempts to obtain the locale from the device. If that fails, the SIP trunk attempts to obtain the user locale from the Common Device Configuration and if that fails, the SIP trunk obtains the user locale that is used for the Enterprise Parameters.

Incorrect Note about User Locales

This documentation update resolves CSCuq42434.

The note about user locales in the Cisco Unified IP Phone settings section of the *Administration Guide* incorrectly states that Cisco Unified Communications Manager uses the user locale that is association with the device pool. The following is the correct note:

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the common device configurations.

Cisco Unified Communications Manager Bulk Administration Guide

CSCui06050 Model is Not a Valid Device Field When Generation a Phone Report

The Phone Reports section mentions Model as one of the fields. However, this field is not available in the Bulk Administration Tool GUI.

CSCul78860 BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials

The table in “End user digest credential settings” sub section of “Digest authentication for SIP phones setup” section states that Digest Credentials accepts alphanumeric characters, which is wrong. The Digest Credentials accepts only hexadecimal characters for BAT User Template.

Cisco Unified Communications Manager TCP and UDP Port Usage

There is an error in table 6 of the *Cisco Unified Communications Manager TCP and UDP Port Usage* document. For port 2445, the description should say that the purpose of this port is to provide trust verification service to SCCPS phones. However, the port is also used to provide trust verification to SIP phones.

Missing Information about TCP Port 22

This documentation update resolves CSCus05634.

The following entry is omitted from the ‘Intracluster Ports Between Cisco Unified Communications Manager Servers’ table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager.*

From (Sender)	To (Receiver)	Destination Port	Purpose
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP service. You must open this port when installing a new subscriber.

Cisco Unified Serviceability Administration Guide

The Cisco Unified Serviceability Administration Guide contains the following updates:

- Audit Log Severity Levels, page 92
- CSCun47221 Note added to the CDR Repository Manager section, page 93
- Missing Information about the Platform Administrative Web Service, page 93

Audit Log Severity Levels

The following table describes the severity levels for audit log messages.

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

CSCun47221 Note added to the CDR Repository Manager section

The following note has been added to the 'CDR Repository Manager' section:

Note When FIPS mode is enabled, CDR files are unable to transfer successfully from subscriber nodes to the publisher node. For assistance in resolving this problem, contact Cisco Technical Assistance Center (TAC).

Missing Information about the Platform Administrative Web Service

This documentation update resolves CSCup84833

The following information is omitted from the Platform Services Section of the *Cisco Unified Serviceability Administration Guide*:

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Note Do not activate the Platform Administrative Web Service on the PAWS-M server.

Troubleshooting Guide for Cisco Unified Communications Manager

In the “Performing Failed RAID Disk Replacement Without Restart” procedure in the *Troubleshooting Guide for Cisco Unified Communications Manager*, step 10 is incorrect. It should read as follows:

10. To check the RAID rebuild status, perform the following steps:

a. Check the LED on the disk. When the rebuild completes successfully, the LED changes from flashing amber to green.

b. Check the status of the physical disk by entering the show hardware CLI command.

A “State Optimal” message appears under the Logical Drives Information section.

c. Check a generated syslog. To generate a syslog, see the “Schedule trace collection” topic in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

A “Rebuild complete” message appears.

Kerneldump utility

The “Netdump utility” section in the *Troubleshooting Guide for Cisco Unified Communications Manager* is replaced with the following “Kerneldump utility” section:

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiringa secondary server.

In a Cisco Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Cisco Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade Cisco Unified Communications Manager from supported appliance releases.

Caution Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The command line interface (CLI) for the Cisco Unified Communications Operating System can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Configuring the kerneldump utility

Step 1 To configure the kerneldump utility on a CUCM node, start a CLI session as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 To view the status of the kerneldump utility, execute the **utils os kerneldump server status** command.

Step 3 If the status of the kerneldump utility is disabled, execute the **utils os kerneldump server start** command. This will require a node restart, so do not execute this command during production hours.

Working with files that are collected by the kerneldump utility

To view the crash information from the kerneldump utility, use the Cisco Unified Real-Time Monitoring Tool or the command line interface (CLI). To collect the kerneldump logs by using the Cisco Unified Real-Time Monitoring Tool, choose the Collect Files option from Trace & Log Central. From the **Select System Services/Applications** tab, choose the **Kerneldump logs** check box. For more information on collecting files using Cisco Unified Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*

To use the CLI to collect the kerneldump logs, use the “file” CLI commands on the files in the crash directory. These are found under the “activelog” partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Cisco Unified Communications Manager System Guide

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

- SMDI Voice Mail Integration, page 95
- Updates to section Phones that Support International Escape Character +, page 95

SMDI Voice Mail Integration

These updates apply to the SMDI Voice Mail Integration section in *Cisco Unified Communications Manager System Guide*.

To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager, use a ATEN USB Serial Converter UC-232A adapter.

For SMDI integration, the FXS port must be configured as a POTS line. If you are not able to configure it in the Route Group, follow the below configuration steps:

1. Configure the Line Group with the FXS port. See “Line Group Configuration” in *Cisco Unified Communications Manager Administration Guide* for more detailed information.
2. Configure the Hunt List (With VoiceMail Usage selected). See “Hunt List Configuration” in *Cisco Unified Communications Manager Administration Guide* for more detailed information.
3. Configure the Hunt Pilot with the voicemail number. See “Hunt Pilot Configuration” in *Cisco Unified Communications Manager Administration Guide* for more detailed information.

Updates to section Phones that Support International Escape Character +

The up-to-date list of phones that support International Escape Character is as follows:

- Cisco Unified SIP Phones 3900 Series (3905, 3911)
- Cisco Unified IP Phones 6900 Series (6921, 6941, 6961, 6945)
- Cisco Unified IP Phones 7900 Series (7942, 7945, 7962, 7965, 7975, 7931)
- Cisco Unified IP Phones 8800 Series (8831)
- Cisco Unified IP Phones 8900 Series (8941, 8945, 8961)
- Cisco Unified IP Phones 9900 Series(9951, 9971)

EX60, EX90, MX200, MX300

Cisco Unified Communications Manager Security Guide

- CUMA Acronym, page 96
- Roll back cluster to a pre-8.0 release section update, page 96
- Refresh Upgrade update, page 96
- CSCuj71412 Secure Call Monitoring and Recording Update, page 96
- CSCuo01831 Phone Models Supporting Encrypted Configuration File, page 96
- CSCus63274 Devices Reset After Certificate Regeneration, page 97
- Incorrect Configuration Example for ASA Router, page 97

CUMA Acronym

In the *Cisco Unified Communications Manager Security Guide, the expansion of the acronym CUMA is incorrect. The correct expansion is Cisco Unified Mobility Advantage.*

Roll back cluster to a pre-8.0 release section update

The note in step 1 of "Roll back cluster to a pre-8.0 release" section incorrectly stated "pre-8.6". This is now changed to "pre-8.0".

Refresh Upgrade update

The following information is missing from the "Refresh upgrade from Cisco Unified Communications Manager Release 7.x to Release 8.6 or later" section in *Cisco Unified Communications Manager Security Guide*:

Once the publisher is up after the upgrade, do not reboot until the CAR migration completes. You are not allowed to switch to old version or perform a DRS backup in this phase. You can monitor the CAR migration status by navigating to **Cisco Unified Serviceability > Tools > CDR Analysis and Reporting**.

CSCuj71412 Secure Call Monitoring and Recording Update

The note in the "About secure call monitoring and recording setup" section is updated to remove the word "Secure" as the system does not support recording on authenticated phones.

Note The system does not support recording on authenticated phone.

CSCuo01831 Phone Models Supporting Encrypted Configuration File

The phone models support table is missing entries. The following table lists all support phone models:

You can encrypt the phone configuration file for the following Cisco Unified IP Phones.

Phone Model and Support	Encryption Method
Cisco Unified IP Phone 7905G or 7912G (SIP only)	Manual key distribution—Encrypt ion algorithm: RC4Key size: 256 bits File signing support: No

Phone Model and Support	Encryption Method
Cisco Unified IP Phone 7940G or 7960G (SIP only)	Manual key distribution—Encryption algorithm: Advanced Encryption Standard (AES) 128Key size: 128 bits File signing support: These phones that are running SIP receive signed, encrypted configuration files but ignore the signing information.
Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961 Cisco Unified IP Phone 7970G, 7971G, or 7975G; Cisco Unified IP Phone 7961G, 7962G, or 7965G;Cisco Unified IP Phone 7941G, 7942G, or 7945G;Cisco Unified IP Phone 7911G; Cisco Unified IP Phone 7906G Cisco Unified IP Phone 7971G-GE, 7961G-GE, 7941G-GE Cisco Unified IP Phone 7931G, 7921G, 7925G, 7926G (SCCP only) Cisco Unified IP Phone 8941 and 8945 Cisco Unified IP Phone 8961, 9951, and 9971	Symmetric key encryption with phone public key (PKI encryption)—Encryption algorithm: AES 128Key size: 128 bits File signing support: Yes

CSCus63274 Devices Reset After Certificate Regeneration

Note All the devices (phones) reset when you regenerate TVS/ CCM/ CAPF client application certificates.

Incorrect Configuration Example for ASA Router

This documentation update resolves CSCuv20903.

The “Set up ASA for VPN Client on IP Phone” procedure in the “VPN Client” chapter provides an example to configure an IOS router instead of an ASA router.

The following procedure contains the correct example.

Procedure

Step 1 Complete the local configuration.

a. Configure network interface.

Example:

ciscoasa(config)# **interface Ethernet0/0**

ciscoasa(config-if)# **nameif outside**

ciscoasa(config-if)# **ip address 10.89.79.135 255.255.255.0**

ciscoasa(config-if)# **duplex auto**

ciscoasa(config-if)# **speed auto**

ciscoasa(config-if)# **no shutdown**

ciscoasa#**show interface ip brief** (shows interfaces summary)

b. Configure static routes and default routes.

ciscoasa(config)# route <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

ciscoasa(config)# **route outside 0.0.0.0 0.0.0.0 10.89.79.129**

c. Configure DNS.

Example:

ciscoasa(config)# **dns domain-lookup inside**

ciscoasa(config)# **dns server-group DefaultDNS**

ciscoasa(config-dns-server-group)# **name-server 10.1.1.5 192.168.1.67209.165.201.6**

Step 2 Generate and register the necessary certificates for Cisco Unified Communications Manager and ASA. Import the following certificates from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Cisco Unified Communications Manager certificates, do the following:

a. From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

b. Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as a .txt file.

c. Create trustpoint on the ASA.

Example:

ciscoasa(config)# **crypto ca trustpoint trustpoint_name**

ciscoasa(ca-trustpoint)# **enrollment terminal**

ciscoasa(config)# **crypto ca authenticate trustpoint_name**

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d. Generate the following ASA self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

ciscoasa> **enable**

ciscoasa# **configure terminal**

ciscoasa(config)# **crypto key generate rsa general-keys label <name>**

ciscoasa(config)# **crypto ca trustpoint <name>**

ciscoasa(ca-trustpoint)# **enrollment self**

ciscoasa(ca-trustpoint)# **keypair <name>**

ciscoasa(config)# **crypto ca enroll <name>**

ciscoasa(config)# **end**

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.

  Example:

ciscoasa> **enable**

ciscoasa# **configure terminal**

ciscoasa(config)# **crypto key generate rsa general-keys label <name>**

ciscoasa(config)# **crypto ca trustpoint <name>**

ciscoasa(ca-trustpoint)# **enrollment self**

ciscoasa(ca-trustpoint)# **fqdn <full domain name>**

ciscoasa(config-ca-trustpoint)# **subject-name CN=<full domain name>,CN=<IP>**

ciscoasa(config)# **crypto ca enroll <name>**

ciscoasa(config)# **end**

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

ciscoasa(config)# **crypto ca export <name> identity-certificate**

Copy the text from the terminal and save it as a .pem file and upload it to the Cisco Unified Communications Manager.

Step 3 Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

ciscoasa(config)# **username CP-7975G-SEP001AE2BC16CB password**

k1kLGQIoxyCO4ti9 encrypted

ciscoasa(config)# **username CP-7975G-SEP001AE2BC16CB attributes**

ciscoasa(config-username)# **vpn-group-policy GroupPhoneWebvpn**

ciscoasa(config-username)#**service-type remote-access**

Cisco Unified Communications Manager Operating System Administration Guide

In the online version of the *Cisco Unified Communications Manager Operating System Administration Guide*, the "Software Upgrade Considerations" section contains an error in the list of topics that are included in that section. The list includes a link to a topic called "Upgrading to Cisco Unified Communications Manager Release 8.0(1) or Later from Release from Release 7.x;" this topic does not exist and the link to it is therefore broken. The list should read as follows:

This section contains the following topics:

- Overview of the Software Upgrade Process
- Making Configuration Changes During an Upgrade
- Upgrading a Cluster in Parallel
- Supported Upgrades
- Obtaining the Upgrade File
- Supported SFTP Servers

This error does not occur in the PDF version of the guide.

Cisco Unified Real-Time Monitoring Tool Administration Guide

The following alerts have been removed from Unified CM but are still listed in the *Cisco Unified Real Time Monitoring Tool Administration Guide*:

LowAttendantConsoleServerHeartbeatRate

LowCallManagerHeartbeatRate

LowTFTPServerHeartbeatRate

Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert

This documentation update resolves CSCuq39087

The default threshold value for LogPartitionLowWaterMarkExceeded alert is incorrectly described as 95% in the "Alerts" chapter. The following table contains the correct value.

Value	Default Configuration
Threshold	Trigger alert when following condition is met: Log Partition Used Disk Space Exceeds Low Water Mark (90%)

Cisco Unified Communications Manager TCP and UDP Port Usage

Incorrect LDAP Port Information

This guide incorrectly lists the destination port from Unified Communications Manager to External Directory as Ephemeral.

Unified Communications Manager to External Directory is 389 LDAP, 636 for secure LDAP, or 3269 for global catalog. External Directory to Unified Communications Manager is Ephermeral.

The following table shows the correct ports between Unified Communications Manager and LDAP directory.

From (Sender)	To (Listener)	Destination Port	Purpose
Unified CM	External Directory	389, 636, 3628, 3629 / TCP	Lightweight Directory Access Protocol (LDA query to external direc (Active Directory, Net Directory)
External Directory	Unified CM	Ephemeral	

Command Line Interface Reference Guide

The following change exists for the Command Line Interface Reference Guide:

show perf query counter Command Output

This documentation update resolves CSCuo70238.

The following note is omitted from the show perf query counter command section in the *Cisco Unified Communications Command Line Interface Guide*.

The output that this command returns depends on the number of endpoints that is configured in the Route Groups in Cisco Unified Communications Manager.

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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2011 Cisco Systems, Inc. All rights reserved.