# Release Notes for Cisco Unified Communications Manager Release 8.5(1)

**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 8.5(1) Release Notes***

| Date | Change |
|---|---|
| 6-22-16 | Added Outdated Information for Auto-Attendant, page 46. |
| 3-11-16 | Added Directory Number Field Description Updated, page 71. |
| 2-01-16 | Added Domain Name Change for Cisco Unified Communications Manager, page 52. |
| 1-14-16 | Added Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 18. |
| 6-30-2015 | Added Correction in Software Conference Bridge Maximum Audio Streams, page 53 |
| 4-14-2015 | Added FAC and CMC Code is not Captured in CDR, page 65. |
| 3-10-2015 | Added Incorrect Order of CDR and CMR Fields, page 64. |
| 2-16-2015 | Added Incorrect CDR Field Description for destCallTerminationOnBehalfOf, page 64. |
| 1-8-2015 | Added Supported SFTP Servers to System Requirements, page 3. |
| 11-04-2014 | Added Incorrect Note about User Locales, page 55. |
| 10-07-2014 | Added Missing Information about the Platform Administrative Web Service, page 62. |

**Cisco Systems, Inc.**
www.cisco.com

*Table 1 Updates to Release Notes for Cisco Unified Communications Manager 8.5(1) Release Notes*

| Date | Change |
|---|---|
| 9-19-2014 | Added show perf query counter Command Output, page 71. |
| 9-5-2014 | Added Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert, page 67. |
| 6-27-2014 | Added CSCtd43582 Remote Destination and Auto Answer, page 45. |
| 6-9-2014 | Added CSCuo97956 Unified CM8.5 documentation doesn't mention unrestricted VPN support, page 68. |
| 6-3-2014 | Added CSCup04321 Call Pickup Group Visual Notification does not Support Localization, page 45. |
| 5-16-2014 | Added CSCuo10697 Updated List of LDAP Supported Directories, page 45. |
| 4-30-2014 | Added CSCuo13148 Cisco ATA 187 Analog Telephone Adaptor Compatibility, page 45. |
| 4-10-2014 | Added Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 18. |
| 3-13-2014 | Added CSCul78860 BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials, page 60. |
| 10-15-2013 | Added Updates to section Phones that Support International Escape Character +, page 60 to Documentation Updates. |
| 10-11-2013 | Added Added description for For voice mail usage option in Add hunt list procedure, page 55 to Documentation Updates. |
| 09-25-13 | Added a note about using externally powered USB to upgrade prerequisites. |
| 08-29-13 | Added CSCug84842 Installation fails with unrecoverable internal error, page 44 to Important Notes. |
| 08-06-13 | Added CSCui06050 Model is Not a Valid Device Field When Generation a Phone Report, page 60 to Documentation Updates. |
| 06-03-13 | Added Removed field Call Stats from SIP Profile configuration, page 55 to Documentation Updates. |
| 04-09-13 | Added CSCuf57901 Video resolution support for SIP phones, page 19 to Important Notes. |
| 01-29-13 | Added CSCub12922 Adding a new subscriber causes device reset, page 19 to Important Notes. |
| 01-21-13 | Added CSCud95087 Limitation of SIP Forking on Trunk Not Documented, page 35 to Important Notes. |
| 01-07-13 | Added missing table entry for Cisco Unified Communications Manager Call Detail Records Administration Guide, page 64 to Documentation Updates. |
| 01-04-13 | Added CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 34 to Important Notes. |
| 01-02-13 | Added CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT, page 20 to Important Notes. |

# Contents

This document includes the following information:


- Introduction, page 3
- System Requirements, page 3
- Upgrading to Cisco Unified Communications Manager 8.5(1), page 6
- Related Documentation, page 15
- Important Notes, page 16
- New and Changed Information, page 46
- Caveats, page 46
- Documentation Updates, page 51
- Obtaining Documentation and Submitting a Service Request, page 71


Before you install or upgrade Cisco Unified Communications Manager, Cisco recommends that you review the "Upgrading to Cisco Unified Communications Manager 8.5(1)" section on page 6, for information pertinent to installing or upgrading, and the "Important Notes" section on page 16 for information about issues that may affect your system.

# Introduction

Cisco Unified Communications Manager, 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 Cisco Unified Communications Managers worldwide. Cisco has obtained an unrestricted US export classification for Cisco Unified Communications Manager.

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

# System Requirements

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

### Server Support

Make sure that you install and configure Cisco 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 Cisco Unified CM, refer to the Supported Servers for Cisco Unified Communications Manager 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 Cisco Unified CM Release 8.5(1).

**Note** Be aware that some servers that are listed in the *Cisco Unified Communications Manager Software Compatibility Matrix* may require additional hardware support for Cisco Unified CM Release 8.5(1). 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 Cisco Unified Communications Manager

Cisco recommends that you connect each Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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 Universal Serial Bus (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 Cisco Unified Communications Manager releases, MCS models and/or UPS vendor/make/models, you can cause an external script to monitor the UPS. When low battery gets detected, you can log on to Cisco Unified Communications Manager 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 |

*Table 2 Supported Servers for UPS Integration (continued)*

| HP Servers | IBM Servers | UCS Servers |
|---|---|---|
| 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, please 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.<br><br>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:<br><br>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.<br><br>Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions.<br><br>For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner. |

# Upgrading to Cisco Unified Communications Manager 8.5(1)

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


- Before You Begin, page 6
- Special Upgrade Information, page 7
- Upgrade Paths, page 9
- Ordering the Upgrade Media, page 10
- Latest Software and Firmware Upgrades for Unified CM 8.5 on Cisco.com, page 15
- Upgrading to Restricted Cisco Unified Communications Manager 8.5(1), page 10
- Upgrading to Unrestricted Cisco Unified Communications Manager 8.5(1), page 11
- Upgrading from a Local Source, page 12
- Upgrading from a Remote Source, page 13


## Before You Begin

In Cisco Unified Communications Manager 8.5(1), the image available for download from Cisco.com is a non-bootable image that can only be used for upgrades. Cisco Unified Communications Manager 8.5(1) upgrade DVDs ordered from Cisco are bootable and can be used for upgrades or fresh installs.

**Note** Follow the install instructions located here:

http://www.cisco.com/en/US/customer/docs/voice_ip_comm/cucm/install/8_5_1/install/cmins851.html

1. Before you upgrade the software version of Cisco Unified Communications Manager, verify your current software version.

   To do that, open Cisco Unified Communications Manager Administration. The following information displays:

   - Cisco Unified Communications Manager System version
   - Cisco Unified Communications Manager Administration version

2. Read the "Special Upgrade Information" section on page 7.

**Note** Cisco recommends that you remove the bootable DVD from the DVD drive after an upgrade. If you reboot your system with the bootable DVD in the drive, your disk may be reformatted. At the completion of the upgrade, the DVD ejects. Confirm that the DVD ejected and remove the DVD physically from the DVD drive.

**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.

**Note** When you upgrade the Cisco Unified Communication Manager cluster, you must restart the Cisco Unified Mobility Advantage server to ensure it can register mobile clients.

**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.

# Special Upgrade Information

The following sections include information that you must know before you begin the upgrade process.


- Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before Upgrade, page 8
- Update the CTL client, page 8
- Do Not Make Configuration Changes During an Upgrade, page 8

## Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before Upgrade

Before you upgrade to Cisco Unified Communications Manager 8.5(1), ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters in Cisco Unified Communications Manager Administration. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail when you upgrade to Cisco Unified Communications Manager8.5(1) and the following error message gets written to the upgrade log:

```
InstallFull *ERROR* Name for Cisco Unified Mobile Communicator device(s) must be 15 or
less, please correct and rerun upgrade.
```

If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters before the upgrade.

## Update the CTL client

When you upgrade to Cisco Unified Communications Manager 8.5(1) from a release prior to 7.1(5), you must update the Certificate Trust List (CTL) client. Updating the CTL client ensures that phones can accept configuration updates after the upgrade is complete. For information about how to update the CTL client, see "Configuring the Cisco CTL client" in the *Cisco Unified Communications Manager Security Guide 8.5(1)*.

## Do Not Make Configuration Changes During an Upgrade

Do 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.

If you are upgrading your system, 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, you have switched the servers over to the upgraded partition, and 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).

**Tip** For detailed information about the upgrade process, see the "Software Upgrades" chapter, in the *Cisco Unified Communications Operating System Administration Guide*.

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

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

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

**Step 5** Switch 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 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 Real Time Monitoring Tool Administration Guide*.

**Step 7** When all other upgrade tasks are complete, you can perform configuration tasks.

# Upgrade Paths

For information about supported Cisco 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

**Note** The *Cisco Unified Communications Manager Software Compatibility Matrix* incorrectly lists Release 7.1(5b)SU4 as a direct upgrade path for Cisco Unified CM Release 8.5.1.10xxx-xx and 8.5.1.11xxx-x. Direct upgrades to these releases from Release 7.1(5b)SU4 are not supported.

# Ordering the Upgrade Media

To upgrade to Cisco Unified CM Release 8.5(1) 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 Cisco Unified Communications Manager, you must purchase the upgrade from Cisco Sales.

For more information about supported Cisco 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*.

# Upgrading to Restricted Cisco Unified Communications Manager 8.5(1)

This section contains instructions for upgrading to the restricted version of Cisco Unified Communications Manager 8.5(1)


- Upgrading from Unified CM 6.x or Later by Using the UCSInstall ISO File, page 10


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

**Note** Release 6.x customers can install this version, but the ccm.exe will not run unless 7.0 software licenses exist on the system.

Because of its size, the UCSInstall iso file, UCOS_8.5.1.10000-26.sgn.iso, comprises three parts:

- UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part1of3
- UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part2of3
- UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part3of3

**Procedure**

**Step 1** From the Software Download page on Cisco.com, download the three UCSInstall iso files.

**Step 2** To combine the three files, execute one of the following commands.

**Note** Because the UCSInstall_UCOS_8.5.1.10000-26 build specifies a nonbootable ISO, the build proves useful only for upgrades. You cannot use this build for new installations.

**a.** If you have a Unix/Linux system, enter (copy and paste) the following command into the CLI:

cat UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part1of3 UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part2of3 UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part3of3 > UCSInstall_UCOS_8.5.1.10000-26.sgn.iso

**b.** If you have a Windows system, enter (copy and paste) the following command into the command prompt (cmd.exe):

COPY /B
UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part1of3+UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part2of3+UCSInstall_UCOS_8.5.1.10000-26.sgn.iso_part3of3
UCSInstall_UCOS_8.5.1.10000-26.sgn.iso

**Step 3** Use an md5sum utility to verify that the MD5 sum of the final file is:

0c32c562fce5b5be5d9b8f01c749b63f UCSInstall_UCOS_8.5.1.10000-26.sgn.iso

**Step 4** Continue by following the instructions in the "Upgrading from a Local Source" section on page 12 or the "Upgrading from a Remote Source" section on page 13.

# Upgrading to Unrestricted Cisco Unified Communications Manager 8.5(1)

**Note** The unrestricted version of Unified CM 8.5(1) 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 will not even be allowed to fresh install a restricted version on a system that contains an unrestricted version.

This section includes the following information:

- Installing the Unrestricted COP File, page 11
- To see if your current version of Cisco Unified Communications Manager is compatible with the unrestricted version of Cisco Unified Communications Manager 8.5(1), see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html, page 11

## Installing the Unrestricted COP File

Before you upgrade from Compatible Versions of Cisco Unified Communications Manager 5.1(3x), 6.x or 7.x to unrestricted Cisco Unified Communications Manager 8.5(1), install the unrestricted COP file (**ciscocm.allow_upgrades_to_unrestricted.cop.sgn**) that you can find under:

Cisco Unified Communications Manager Version 8.5 -> Unified Communications Manager / CallManager / Cisco Unity Connection Utilities -> COP-Files

### Compatible Versions

To see if your current version of Cisco Unified Communications Manager is compatible with the unrestricted version of Cisco Unified Communications Manager 8.5(1), see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

## Upgrading from Unified MC 6.x or Later by Using the UCSInstall File

**Note** Release 6.x customers can install this version, but the ccm.exe will not run unless 8.0 software licenses exist on the system.

Because of its size, the UCSInstall iso file comprises three parts:

- UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part1of3
- UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part2of3
- UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part3of3

**Procedure**

**Step 1** Ensure that you have completed the "Installing the Unrestricted COP File" section on page 11.

**Step 2** From the Software Download page on Cisco.com, download the three UCSInstall files.

**Step 3** To combine the files, execute one of the following commands.

**Note** Because the UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso build specifies a nonbootable ISO, the build proves useful only for upgrades. You cannot use this build for new installations.

**a.** If you have a Unix/Linux system, copy and paste the following command into the CLI:

```
cat UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part1of3 UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part2of3
    UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part3of3 > UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso
```

**b.** If you have a Windows system, copy and paste the following command into the command prompt (cmd.exe):

```
COPY/B
UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part1of3+UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_
part2of3
+UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso_part3of3 UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso
```

**Step 4** Use an md5sum utility to verify that the MD5 sum of the final file is correct.

3be0a3815a1b7fb572e91bd0df565b05 UCSInstall_UCOS_UNRST_8.5.1.10000-26.sgn.iso

**Step 5** Continue by following the instructions in the "Upgrading from a Local Source" section on page 12 or the "Upgrading from a Remote Source" section on page 13.

# Upgrading from a Local Source

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

**Procedure**

**Step 1** 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 2** Insert the new DVD into the disc drive on the local server that is to be upgraded.

**Step 3** Log in to Cisco Unified Communications Operating System Administration.

**Step 4** Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

**Step 5** From the **Source** list, choose **DVD**.

**Step 6** Enter a slash (/) in the Directory field.

**Step 7** To continue the upgrade process, click **Next**.

**Step 8** Choose the upgrade version that you want to install and click **Next**.

**Step 9** In the next window, monitor the progress of the install.

**Step 10** Perform one of the following procedures:

a. To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and is running the upgraded software

or

b. To install the upgrade and manually reboot to the upgraded partition at a later time, do the following steps:

1. Choose **Do not reboot after upgrade**.
2. Click **Next**.
3. The Upgrade Status window displays the Upgrade log.
4. When the installation completes, click **Finish**.
5. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts, running the upgraded software.

# Upgrading from a Remote Source

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

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

### Procedure

**Step 1** Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

a. If you have a Cisco-provided upgrade disk, copy the contents of the disk to the remote server.

b. If you downloaded the upgrade files, copy the files you downloaded to the remote server.

**Step 2** Log in to Cisco Unified Communications Operating System Administration.

**Step 3** Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

**Step 4** From the **Source** list, choose **Remote Filesystem**.

**Step 5** 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 6** In the **Server** field, enter the server name or IP address.

**Step 7** In the **User Name** field, enter your user name on the remote server.

**Step 8** In the **User Password** field, enter your password on the remote server.

**Step 9** Select the transfer protocol from the **Transfer Protocol** field.

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

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

- If you are upgrading from Cisco Unified Communications Manager Release 6.x or 7.x, the upgrade file has the extension sgn.iso.

**Step 12** 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 Cisco Unified Real Time Monitoring Tool.

**Step 13** Perform one of the following procedures:

**a.** To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and is running the upgraded software

or

**b.** To install the upgrade and manually reboot to the upgraded partition at a later time, do the following steps:

1. Choose **Do not reboot after upgrade**.
2. Click **Next**.
3. The Upgrade Status window displays the Upgrade log.

4. When the installation completes, click **Finish**.
5. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts, running the upgraded software.

# Latest Software and Firmware Upgrades for Unified CM 8.5 on Cisco.com

After you install or upgrade to this release of Cisco Unified Communications Manager, 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 Cisco Unified Communications Manager 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 85(1) at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_5_1/rel_notes/ime-rel_notes-851.html.

# Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 8.5(1) as part of Cisco Unified Communications System Release 8.x testing, see

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

**Note** Be aware that the release of Cisco IP telephony products does not always coincide with Cisco Unified Communications Manager releases. If a product does not meet the compatibility testing requirements with Cisco Unified CM, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified Communications Manager Release 8.5(1). For the most current compatibility combinations and defects that are associated with other Cisco 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 Cisco Unified Communications Manager Release 8.5(1).


- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 18
- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 18
- CSCuf57901 Video resolution support for SIP phones, page 19
- CSCub12922 Adding a new subscriber causes device reset, page 19
- CSCtu18692 CallProcessingNodeCpuPegging Alerts During DRF/BAT, page 20
- CSCud38747 directory-trust No Longer Security Certificate Option, page 20
- CSCtb31860 Transcoding G.711 to All Codecs Supported, page 20
- CSCtr78911 Answer Too Late Timer, page 20
- CSCts83374 Remote Destination Configuration Settings for Single Number Reach and Reroute Remote Destination Calls to Enterprise Number, page 20
- CSCto57498 Upgrading to Cisco Unified Communications Manager Release 8.x from Release 7.x, page 21
- CSCtd69640 Downtime when upgrading Publisher server until all Subscriber servers are updated, page 22
- CSCtk68384 Disable ICH10 onboard SATA controller on EX/ESXi servers during Unified CM installation, page 22
- CSCub10861 Call waiting behavior with MLPP Preemption correction, page 22
- CSCua01779 Cisco Unified Communications Manager Locale Installer locale file for Belgium, page 23
- CSCtz88812 Cisco IP Phones and Cisco Unity Connection support for IPv6, page 23
- CSCte39796 Increase database replication timeout when upgrading large clusters, page 23

- CSCsy57492 Hold Reversion Notification Interval for SCCP and SIP phones, page 23
- New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651), page 24
- CSCtn32528 MLPP feature support only for SCCP phones, page 24
- CSCtn50405 CUCM DRF Backup does not backup certificates, page 24
- Unrestricted Release Limitations, page 24
- CSCtd87058 BAT Impact, page 24
- Limitations to Call Park Feature, page 25
- CSCth53322 Rebuild Server After You Use the Recovery Disk, page 26
- Verify IPv6 Networking on Servers Before Upgrade, page 26
- CSCte05285 IBM I3 Servers Automatic Server Restart (ASR) Default Specifies Disabled, page 26
- Disaster Recovery System Caution, page 27
- EMCC Login Affects Settings in Product-Specific Configuration Layout of Phone Configuration Window, page 27
- CSCtl05204 Cisco Unified CM Cored for Call Forwarding for all Scenarios with Early Offer Configured on a SIP Trunk, page 27
- CSCtl47624 No Music On Hold when using ASR 1000, page 27
- CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value, page 28
- CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters, page 28
- CSCtr62446 Route List Run on All Nodes Service Parameter, page 28
- CSCtr89029 URL Parameters for Secured Phones Repopulated After Restart, page 28
- CSCtr84167 Block Offnet to Offnet Transfer, page 28
- CSCtr21486 Troubleshooting Guide Update to Switch Version, page 28
- CSCtg67435 Certificate Regeneration During Domain Name Change, page 29
- CSCtr007539 MDCX Sendonly Message Suppressed for MGCP Calls, page 29
- CSCtf48747 DTMF Suppressed When G.Clear is Advertised, page 29
- CSCtw25693 MoH Does Not Support DTMF, page 29
- CSCte44108 Call Control Discovery Limitation, page 29
- CSCte43366 Japanese characters displayed as "_" in Music On Hold File, page 29
- CSCtx00678 Do not use Voicemail for Alerting Name or ASCII Alerting Name, page 30
- CSCtx86215 Database Replication, page 30
- CSCtf53999 Single Fixed Music on Hold Source Per Cluster, page 30
- CSCsu23100 Missing Information on Special Characters, page 30
- CSCtx92282 Cisco Unified IP Phones 9951 and 9971 Support SIP Dial Rules, page 30
- CSCty75069 Secured Directory URL Enterprise Parameter overrides Directory field in Phone Configuration, page 31
- CSCtr44481 Download Dial Plans for Cisco Unified Communications Manager Release 8.X, page 31
- CSCty16160 During publisher node restores DB replication status must be 2 before you reboot the cluster, page 31

- CSCtz73477 Interactions with Call Forward iDivert and Voice-Messaging features, page 31
- CSCtu52978 Hard disk replacement fails if write cache is enabled on Cisco MCS 7828/28-i3, page 31
- CSCth80282 Update regenerate certificate in Unified CM Operating System Guide, page 32
- CSCtw78204 RTMT cannot collect OPC logs under default settings, page 32
- CSCtc71174 Call Park and Directed Call Park Restriction, page 32
- CSCtg71595 Allowed characters for Cluster ID field, page 33
- CSCub12688 FinalCalledPartyNumber CDR field description, page 33
- CSCuc10415 Tip for Adding a New Server, page 33
- CSCub77698 Cause tag required for convertHITоDiversion() API, page 33
- CSCuc23992 Call Preservation support for SIP trunks, page 33
- 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 34
- CSCud57169 CTL file size limit of 32 kilobytes should be 64 kilobytes, page 34
- CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 34
- CSCud95087 Limitation of SIP Forking on Trunk Not Documented, page 35
- CSCui20049 Restructure of Disaster Recovery Documentation for Restore Scenarios, page 35
- CSCug84842 Installation fails with unrecoverable internal error, page 44
- CSCuo13148 Cisco ATA 187 Analog Telephone Adaptor Compatibility, page 45
- CSCuo10697 Updated List of LDAP Supported Directories, page 45
- CSCup04321 Call Pickup Group Visual Notification does not Support Localization
- 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.

# Perfect Forward Secrecy is not Supported in IPsec Configuration

This information applies to CSCuu74346.

Perfect Forward Secrecy (PFS) security service is not supported in IPsec configuration between Cisco Unified Communications Manager and Voice Gateway.

# 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.

# 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.

# CSCud38747 directory-trust No Longer Security Certificate Option

The directory-trust option is no longer available for uploading Directory Trust certificates using Cisco Unified Communications Operating System Administration. Use the tomcat-trust certificate option instead.

# 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 8.0, 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.

A statement of MLPP feature support is added to the Cisco Unified Communications Manager documentation, versions 9.0 and higher.

# CSCtn50405 CUCM DRF Backup does not backup certificates

Backup files created by DRS do not contain the required certificates to maintain Security By Default functionality after a restore. After restoring for disaster recovery, hardware migration, or bridge upgrade, manually deleting ITL files on phones may be necessary unless an upgrade for this defect is performed before taking a backup. See the Bug Details of fix CSCtn50405 for complete instructions on resolving this issue.

This issue is fixed in Cisco Unified Communications Manager versions 8.5(1)su2 and higher.

# 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.

# CSCtd87058 BAT Impact

If your Cisco 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

# Limitations to Call Park Feature

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 25
- CSCsz31137 Parked Call Gets Reverted When the Parkee is on, page 25
- CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve, page 25
- CSCtb53159 Display Limitation in ConfList, page 26


## 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 Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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.

## Verify IPv6 Networking on Servers Before Upgrade

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

## 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.

## Disaster Recovery System Caution

When you restore your data, the hostname, server IP address, DNS configuration, version, and the deployment type values must match their values during the backup. DRS does not restore across different hostnames, IP addresses, DNS configurations, versions, and deployment types.

## 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.

## CSCtl05204 Cisco Unified CM Cored for Call Forwarding for all Scenarios with Early Offer Configured on a SIP Trunk

Cisco Unified CM may crash or call may fail when Early Offer is enabled on a SIP trunk and the call is made to a SCCP device next to a SIP trunk registered to a node which is different from the node of the incoming call.

## 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”.

## 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 (#).

## 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.

## 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.

## 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.

## CSCsv64212 Multicast Address Range for Cisco IP Phone Services

For Cisco IP phone services, Cisco recommends that administrators use an IP address range of 225.0.0.0 through 239.255.255.255.

## CSCtr007539 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.

## CSCtf53999 Single Fixed Music on Hold Source Per Cluster

The music on hold server supports one fixed-device stream source in addition to the file stream sources. This source represents the fixed audio source, which gets configured in the Fixed MOH Audio Source Configuration window. The fixed audio source gets sourced from a fixed device that uses the local computer audio driver.

For each cluster, you may define one fixed audio source. You must set up the fixed audio source that is configured per cluster on each MOH server. To do so, connect a Cisco USB MOH sound adapter, which must be ordered separately, into the USB port for each MOH server in the cluster that you want to provide the fixed audio source.

**Note** For virtual servers, the Fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Cisco Unified Communications Manager does not support USB when running on VMware. Internal Music On Hold, however, is supported on VMware.

## CSCsu23100 Missing Information on Special Characters

For information on special characters and how they can be used in a dial plan, refer to the Wildcards and Special Characters in Route Patterns and Hunt Pilots topic in the Understanding Route Plans chapter from the Cisco Unified Communications Manager System Guide.

## CSCtx92282 Cisco Unified IP Phones 9951 and 9971 Support SIP Dial Rules

The SIP Dial Rule Configuration Settings section of the Cisco Unified Communications Manager Administration Guide lists the phones that support SIP dial rules. However, the section omits the Cisco Unified IP Phones 9951 and 9971, both of which support SIP dial rules.

## 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.

## CSCtz73477 Interactions with Call Forward iDivert and Voice-Messaging features

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

## 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.

# 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**.

# CSCtw78204 RTMT cannot collect OPC logs under default settings

If you are using Cisco Real-Time Monitoring Tool (RTMT) to monitor Cisco Unified Contact Center Enterprise, RTMT cannot collect OPC logs under the default settings. This issue arises because the default timeout for RTMT log collection is 60 seconds, but the OPC log collection process takes longer.

To resolve the issue, open the *<RTMT_INSTALLATION_FOLDER_PATH>/conf/rtmt.xml* file from the RTMT installation folder and change the value for ReadTimeout to 360. After you make the change, RTMT will be able to collect OPC logs.

# 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.

## CSCtg71595 Allowed characters for Cluster ID field

The Cluster ID field in the EMCC Remote Cluster configuration window supports only alphanumeric characters (a-z, A-Z, 0-9), periods (.), and dashes(-). If you enter another character, such as a space or percent sign, you will receive an http error when you click Update Remote Cluster.

## 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.

## 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.

## CSCub77698 Cause tag required for convertHIToDiversion() API

If you are implementing the convertHIToDiversion() function with SIP Transparency and Normalization, a Diversion header will only be produced if the Histoy-Info header contains a "cause=" tag.

## 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".

# CSCud95087 Limitation of SIP Forking on Trunk Not Documented

The following information is missing from "Understanding Session Initiation Protocol" in the *Cisco Unified Communications Manager System Guide*:

- Cisco Unified CallManager Release 4.x does not accept provisional responses (such as 180 Ringing) from more than five destinations. It does not accept a successful response (200 Ok) from any destination that is not among the first five to respond.
- Cisco Unified CallManager Release 5.x and Cisco Unified Communications Manager Release 6.x do not accept provisional responses (such as 180 Ringing) from more than 20 destinations. They do not accept a successful response (200 Ok) from any destination that is not among the first 20 to respond.

# 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 36
- Restoring the First Node only (Rebuilding the Publisher Alone), page 38
- Restoring the Entire Cluster, page 41
- Restoring Subsequent Cluster Nodes (With or Without Rebuild), page 43

# 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 38. If you intend to rebuild the entire cluster, read the "Restoring the Entire Cluster" section on page 41.

**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 38 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 Unifed Communications Solutions*.

## 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.

## 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 8.5(1)* provides information about new and changed features for release 8.5(1).

To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/8_5_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 Cisco Unified Communications Manager Release 8.0 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 Cisco Unified Communications Manager Release 8.5(1) As of December 6, 2010 describe possible unexpected behaviors in Cisco Unified Communications Manager Release 7.1, which are sorted by component.

**Tip** For more information about an individual defect, click the associated Identifier in the "Open Caveats for Cisco Unified Communications Manager Release 8.5(1) As of December 6, 2010" section on page 48 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 Cisco Unified Communications Manager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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 Cisco Unified Communications Manager Release 8.5(1) As of December 6, 2010" section on page 48 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 46.

**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 on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

## Open Caveats for Cisco Unified Communications Manager Release 8.5(1) As of December 6, 2010

The following information comprises unexpected behavior (as of December 6, 2010) that you may encounter in Release 8.5(1) of Cisco Unified Communications Manager.

*Table 3 Open Caveats for Cisco Unified Communications Manager Release 8.5(1) as of December 6, 2010*

| ID | COMPONENT | HEADLINE |
|---|---|---|
| CSCtn50405 | cpi-cert-mgmt | CUCM DRF Backup does not backup certificates |
| CSCtk06849 | axl | /common - 100% usage - AXL service creates huge catalina.out files |
| CSCth58139 | axl | /common - 100% usage - AXL service creates huge catalina.out files |
| CSCtk13563 | bat | BAT incorrectly changes xpansion Module (AOM) fields to 7916 |
| CSCti96515 | bps-import-export | Bulk Admin Export doesnt work on large dial plan runs out of heap space |
| CSCtk60425 | cdr-management | CDR Repository Manager traces should not print passwords |
| CSCtk14042 | cli | Reverse DNS mismatch - CLI does not display all the PTR records |
| CSCtf37698 | cmcti | Incorrect reason code in ExistingCallEvent for supervisor |
| CSCtj50299 | cmcti | CTIManager Coredump on Inactive Partition Following L2 |
| CSCtk32525 | cm-docs | Administrator name reset command is too vagu |
| CSCti87638 | cm-docs | Cleanup call info when line goes out of service |
| CSCtk05743 | cm-docs | DNS information should be same during restore |
| CSCtk58215 | cm-docs | Addition to docs based on CUMA compatilibity |

*Table 3 Open Caveats for Cisco Unified Communications Manager Release 8.5(1) as of December 6, 2010*

| | | |
|---|---|---|
| CSCtj93467 | cm-docs | RAID configuration for C-210 is missing a couple of things |
| CSCtc66558 | cmui | Dependency Record searches consume java heap space causing Tomcat hang |
| CSCtk52839 | cmui | Getting 404 error on MGCP GW Page |
| CSCte45401 | cmui | CUCM: JPN: hardcoded string in Find and List Music On Hold Audio Files |
| CSCtk55101 | cmui | EMCC Intercluster Service Profile page does not migrated properly |
| CSCtk09926 | cp-callcoverage | non default VM profile always use the default VM profiles mailbox mask |
| CSCtj33840 | cpi-appinstall | During Installation - Unity Connection Message stays for 30 mins |
| CSCtk06087 | cp-ime-services | ASA Liscense Expired |
| CSCtk12050 | cpi-os | Security Issue in OpenSSL |
| CSCte05285 | cpi-os | IBM I3 servers Automatic Server Restart (ASR) not enabled by default |
| CSCtk07156 | cpi-platform-api | "utils diagnose test" hits error "test - tomcat_sessions : Failed" |
| CSCti69234 | cpi-third-party | Security Issue in OpenSSL |
| CSCtk61407 | cpi-third-party | Open SSL Ciphersuite Downgrade and J-PAKE Issues |
| CSCtc87894 | cp-mediacontrol | Video: UCM sends sendRecv instead of recvOnly for video call over ICT |
| CSCtk11184 | cp-mediacontrol | CUCM doesnt know how to handle ORC ACK after send CLC |
| CSCtk13918 | cp-mediacontrol | SCCP to TB E20 though EO SIPT, hold/resume disconnect call |
| CSCtj16922 | cp-mediacontrol | There is one way audio when mtp is inserted over SIP EO trunk |
| CSCth53977 | cp-mediacontrol | No Transmission media event and Sup call go idle on Toggle to WC |
| CSCti45722 | cp-mediacontrol | Local RSVP Agent Greeting Call over SIP-Trunk has wrong reservations |
| CSCth58139 | cp-mediacontrol | sRTP:E2E-No Audio after simultaneuos resume |
| CSCtl05024 | cp-mediacontrol | CUCM cored for call forwarding for all scenario with EO config on SIP trunk |
| CSCti98812 | cp-mediacontrol | sRTP: EO- One way audio between h323 fxs and authenticated EP |
| CSCtk36669 | cp-mediacontrol | SIP Polycom VSX 3000A is not able to enter HQ and HD conference |
| CSCti92815 | cp-mediacontrol | ASR CUBE is not sending TCS for Invite (send only) it received |
| CSCtk64428 | cp-mgcp | CCM reset an core with MGCP PRI when receiving unexpected UserUserIE |
| CSCtk14487 | cp-mobility | UCM should CANCEL the DVOR call when DVOR failure happens. |
| CSCtk30494 | cp-mobility | Need to cleanup mTempCalls and Cdfc in several DVO cancel cases |

*Table 3 Open Caveats for Cisco Unified Communications Manager Release 8.5(1) as of December 6, 2010*

| | | |
|---|---|---|
| CSCtk55158 | cp-pri | Calls send from Mobile Voice Access show same calling and called number |
| CSCtk17332 | cp-sccp | After CFA is pressed, Call Pickup fails and ring back tone does not stop |
| CSCtj63163 | cp-sccp | LifeSize no video if call is transfered via audio EP in HD ad-hoc conf |
| CSCtk55956 | cp-sip-station | UCM rejects the unregister with 503 service not avail when port changed |
| CSCtk14531 | cp-sip-station | 3rd party sip phone X-lite registration with CUCM: 7.1.5.10000 |
| CSCtj92502 | cp-sip-trunk | CCM does not relay DTMF digit via SIP Notify to SCCP or CTI endpoints |
| CSCtj91700 | cp-sip-trunk | HQ ad-hoc conference via H.323 ICT trunk has no video |
| CSCtk04861 | cp-sip-trunk | RT phone has no video in sch conference via H.323 trunk |
| CSCtk35141 | cp-sip-trunk | SIP Polycom VSX3000 has no video in scheduled compatibility conference |
| CSCti60031 | cp-sip-trunk | Re-order tone in originating side(CUCM) for unanswered CME call |
| CSCtk60402 | cp-sip-trunk | Calling and called party out of sync when sme and RSVP involved |
| CSCtk52897 | cp-sip-trunk | Transfer MGCP over SIP EO to SIP gw fails in multi node no Xcoder |
| CSCtk77040 | cp-sip-trunk | Intermittent MTP leak in certain SIP call scenarios causes call failures |
| CSCtj95738 | database | PMR 81654 database out of memory while syncing certificate table |
| CSCtj90316 | database-ids | PMR 81134 CUCM Database assert failure after upgrade from 7.1(5) |
| CSCtk08786 | database-ids | Ontape backup manual restore failing - stuck in fast recovery |
| CSCtg09592 | database-ids | PMR 51856 - DRF restore of SUB components dumps DbMon core |
| CSCtj83589 | database-ids | Realize template - failure when already realized |
| CSCtj83600 | database-ids | TableOutOfSync process running while replication still setting up |
| CSCtk16610 | ime-licensing | IME license installation always fail |
| CSCtj68794 | ime-os | Netdump client fails with address resolution error |
| CSCtk62723 | ims | CUPC unable to get desk phone control due to credential policy |
| CSCti00625 | jtapisdk | CallActiveEv intermittently sent instead of CiscoConsultCallActiveEv |
| CSCtk63048 | media_str_app | Buzzing Noise Heard when RTP stream passes through the Sw MTP on CUCM |
| CSCtk35122 | licensing | CUCM License Report shows invalid license |
| CSCtk36409 | sa-database | Inconsistent default settings on Default Usage Profile and User Defined |

*Table 3 Open Caveats for Cisco Unified Communications Manager Release 8.5(1) as of December 6, 2010*

| | | |
|---|---|---|
| CSCtk05418 | sa-mac | Secondary line doesnt route to VM when its in busy/No Answer condition |
| CSCtk64345 | sa-mac | CUCMBE 3000 - Unable to add network subnet |
| CSCtk14729 | sa-maintenance | Backup to Public Shared SFTP server fails |
| CSCtk64764 | sa-platform | CUCMBE 3000 - Unable to generate log file |
| CSCtg79013 | security | tvs core when Pub/Sub1 switch back to old load after Sub2 install on new |
| CSCtc38788 | tapisdk | TAPI Application Stuck - Unable to Start |
| CSCtf07089 | tapisdk | DSCP for QBE packet is not correct on Vista |
| CSCtk15548 | tapisdk | Unable to install a CiscoTSP from a CUCM 7.1.5, on a Windows XP client |
| CSCti53232 | tapisdk | Client keep loading ProviderOpen/Shutdown and causing TSP crash |
| CSCtk05947 | trace-library | CUP PSB testing uncovers missing parameter in SDI call resulting in core |
| CSCtn29923 | CUCMBE 8.5 | IP Address Change Procedure Fails resulting in outage |

# Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Unified Communications Manager release 8.5 documentation suite was released.


- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 52
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 52
- Cisco Unified Communications Manager System Guide, page 59
- Cisco Unified Communications Manager Bulk Administration Guide, page 60
- Cisco Unified Serviceability, page 61
- Cisco Unified IP Phone Services Application Development Notes, page 62
- Disaster Recovery Administration Guide, page 62
- Troubleshooting Guide for Cisco Unified Communications Manager, page 63
- Cisco Unified Communications Manager Call Detail Records Administration Guide, page 64
- Cisco Unified Communications Manager Security Guide, page 68
- Command Line Interface Reference Guide, page 71
- Cisco Unified Communications Manager Online Help, page 71

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


- Domain Name Change for Cisco Unified Communications Manager, page 52


## 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*.

# Cisco Unified Communications Manager Administration

*Cisco Unified Communications Manager Administration Guide*


- Correction in Software Conference Bridge Maximum Audio Streams, page 53
- Correction in Software Conference Bridge Maximum Audio Streams, page 53
- Hub_None Information, page 54
- Clarification of Log Missed Calls Check Box, page 54
- E & M Port Configuration Settings, page 54

- Updated field descriptions for Timer Register Delta and Timer Register Expires, page 54
- Removed field Call Stats from SIP Profile configuration, page 55
- Added description for For voice mail usage option in Add hunt list procedure, page 55
- Incorrect Note about User Locales, page 55

*Cisco Unified Communications Manager System Guide*

- Agent Greeting, page 55
- Whisper Coaching, page 56
- Incorrect Document Reference, page 56

*Cisco Unified Communications Manager Features and Services Guide*

- Suggested MaxConcurrentCallRequests (MCCR) Value, page 56
- Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 56
- Intercom Directory Number Configuration Settings Auto Answer Field is Incorrect, page 57
- Secure Extension Mobility, page 57
- Remote Cluster Menu Path is Incorrect, page 57
- DoCoMo Phones Not Certified, page 58

Cisco Unified Communications Manager Call Detail Records Administration Guide

- CDR Field Descriptions, page 58


## 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

The Trunk Configuration Settings topic in Cisco Unified Communications Manager online help contains an incorrect description of the Parameter Name/Parameter Value field. The updated description is provided below and exists in the *Cisco Unified Communications Manager Administration Guide* on Cisco.com.

> Optionally, enter parameter names and parameter values. Valid values include all characters except equal sign (=), semi-colon (;), and non-printable characters, such as tabs. You can enter a parameter name with no value.
>
> **Example**
>
> | **Parameter Name** | **Parameter Value** |
> |---|---|
> | CCA-ID | 11223344 |
> | pbx | |
> | location | RTP |

You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.

## Hub_None Information

The "Location Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* omits the following information:

The location that is configured in a device pool takes precedence over the location configured in the device when the location in the device is set to Hub_None. If the device location is set to any other user-defined location, standard rules apply and the device parameter takes priority.

## Clarification of Log Missed Calls Check Box

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

## 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.

## 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".

## 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.

## Agent Greeting

The Phone Features section of the "Cisco Unified IP Phones" chapter of the Cisco Unified Communications Manager System Guide omits the following information:

Agent Greeting enables Cisco Unified Communications Manager to automatically play a pre-recorded announcement following a successful media connection to the agent device. The greeting helps keep agents sounding fresh because they do not have to repeat common phrases on each call. Agent Greeting is audible for the agent and the customer.

If you want to use agent greeting, Built-in Bridge must be On.

## Whisper Coaching

The Phone Features section of the "Cisco Unified IP Phones" chapter of the Cisco Unified Communications Manager System Guide omits the following information:

Silent call monitoring is a feature that allows a supervisor to discreetly listen to a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Whisper coaching is an enhancement to the Silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature allows applications to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

## Incorrect Document Reference

The *Cisco Unified Communications Manager System Guide* contains incorrect references to the *Cisco Unified Communications Manager SIP Transparency and Normalization Guide*. The references should be to the *Developer Guide for SIP Transparency and Normalization Guide*.

## Suggested MaxConcurrentCallRequests (MCCR) Value

The Setting Service Parameters for the Webdialer Servlet section of the "Cisco WebDialer" chapter of the *Cisco Unified Communications Manager Features and Services Guide* incorrectly states:

- MCS 7845H2 supports a maximum of 4 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 6 to allow callers to initiate and disconnect calls as needed.

The correct information is:

- MCS 7845H2 supports a maximum of 4 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 8 to allow callers to initiate and disconnect calls as needed.

The same section contains the following information:

The maximum value specifies 6.

The correct information is:

The maximum value specifies 8.

## Setting the Service Parameters for Cisco Unified Communications Manager Assistant

The Setting the Service Parameters for Cisco Unified Communications Manager Assistant section of the "Cisco Unified Communications Manager Assistant With Shared Line Support" and "Cisco Unified Communications Manager Assistant With Proxy Line Support" chapters of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information.

**Note** Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.

## Intercom Directory Number Configuration Settings Auto Answer Field is Incorrect

In the Intercom Directory Number Configuration Settings section of the "Intercom" chapter of the *Cisco Unified Communications Manager Features and Services Guide*, the Auto Answer field description includes an option that no longer exists.

The Auto Answer Off <*Default*> option is no longer available.

## Secure Extension Mobility

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

The Extension Mobility HTTPS Support feature ensures that when communications are exchanged between a Cisco Unified IP Phone service and other applications, that the communications use the HTTPS protocol to ensure that the communications are secure. Users must log into the Cisco Unified CM applications by providing their authentication information. Their credentials are encrypted after the communication protocol changes to HTTPS.

When a visiting Extension Mobility (EM) application fails to locate a user's identification in the local database, the following occurs:

1. Cisco Extension Mobility Cross Cluster (EMCC) sends a request to the local EM service to determine the home cluster of that user (the cluster which owns the user's identification, and which can handle the EM login).
2. The visiting EM service sends a user identification message over HTTPS to all the remote clusters added in the local database.
3. The visiting EM service then parses the response received from the home cluster to get the list of device profiles associated with that user.
   - All further communication between the visiting EM service and home EM service takes place over HTTPS.
   - Similarly, visiting logout requests are also sent from the home EM service to the visiting EM service over HTTPS.

The Extension Mobility HTTPS Support feature is supported on the following IP phones (SIP):

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

**Note** Configure Cisco Extension Mobility on Cisco Unified IP Phones before configuring EMCC.

## 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.

## CDR Field Descriptions

The CDR Field Descriptions table in the *Cisco Unified Communications Manager Call Detail Records Administration Guide* contains errors and omissions relating to video codecs and video resolution fields. The following table shows the corrections:

***Table 4 CDR Field Descriptions***

| Field | Range of Values | Description |
|---|---|---|
| origVideoCap_Codec | 0,<br>100 = H.261,<br>101 = H.263,<br>103 = H.264 | This field identifies the codec type that the originator uses to transmit video (H.261, H.263, or H.264.)<br>Default - 0. If media is not established, this field stays 0. |
| origVideoCap_Resolution | 0,<br>1 = SQCIF,<br>2 = QCIF,<br>3 = CIF,<br>4 = CIF4,<br>5 = CIF16<br>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.<br>Default - 0. If media is not established, this field stays 0. |
| destVideoCap_Codec | 0,<br>100 = H.261,<br>101 = H.263,<br>103 = H.264 | This field identifies the codec type that the terminating party uses to transmit video (H.261, H.263, or H.264).<br>Default - 0. If the destination cannot be reached, this field stays 0. |
| destVideoCap_Resolution | 0,<br>1 = SQCIF,<br>2 = QCIF,<br>3 = CIF,<br>4 = CIF4,<br>5 = CIF16<br>6 = H263 custom resolution | This field indicates the transmitting resolution. In the case of theH.264 codec or a SIP device, this field refers to the max transmitting resolution the device can transmit for this call.<br>Default - 0. If media is not established, this field stays 0. |

| Field | Range of Values | Description |
|---|---|---|
| origVideoCap_Codec_Channel2 | 0,<br>100 = H.261,<br>101 = H.263,<br>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.<br>Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0. |
| origVideoCap_Resolution_Channel 2 | 0,<br>1 = SQCIF,<br>2 = QCIF,<br>3 = CIF,<br>4 = CIF4,<br>5 = CIF16<br>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.<br>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,<br>100 = H.261,<br>101 = H.263,<br>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.<br>Default - 0. If the destination cannot be reached, this field stays 0. |
| destVideoResolution_Channel2 | 0,<br>1 = SQCIF,<br>2 = QCIF,<br>3 = CIF,<br>4 = CIF4,<br>5 = CIF16<br>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.<br>Default - 0. If media is not established, this field stays 0. Also, if H.239 is not supported, this field displays 0. |

# Cisco Unified Communications Manager System Guide

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


- SMDI Voice Mail Integration, page 59
- Updates to section Phones that Support International Escape Character +, page 60


## 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 Bulk Administration Guide

The following changes exist for the *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.

### CSCui78860 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 Operating System Administration

The following changes exist for Cisco Unified Communications Operating System Administration:

- Regenerating a Certificate Update, page 61

## Regenerating a Certificate Update

This update applies to the Regenerating a Certificate procedure in *Cisco Unified Communications Operating System Administration Guide.*

After you regenerate certificates in the Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you must perform restoration tasks for any reason, you must manually unlock each phone in your system so that the phone can register with Cisco Unified Communications Manager. For information about performing a backup, refer to the *Disaster Recovery System Administration Guide*.

# Cisco Unified Serviceability

The following changes exist for Cisco Unified Serviceability documentation.


- Trace Compression, page 61
- Wrong Login URL Included in CAR Documentation, page 61
- Audit Log Severity Levels, page 61
- Missing Information about the Platform Administrative Web Service, page 62


## Trace Compression

The Trace Configuration and Collection Checklist section of the "Understanding Trace" chapter of the *Cisco Unified Serviceability Administration Guide* contains incorrect information regarding trace compression. The correct information follows:

You cannot enable or disable trace compression from an enterprise parameter, the user interface (UI) or the command line interface (CLI).

## Wrong Login URL Included in CAR Documentation

The Logging On to CAR section of the "Configuring the CDR Analysis and Reporting Tool" chapter of the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide contains an incorrect link for logging on to CAR. The correct URL is:*

**https://<Server-ip/name>:8443/car/**

## 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 |

| Severity Code | Description |
|---|---|
| 5 | Notice: normal but significant condition |
| 6 | Informational: informational messages |
| 7 | Debug: debug-level messages |

### 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.

## Cisco Unified IP Phone Services Application Development Notes

The following changes exist for Cisco Unified IP Phone Services Application Development Notes:


- Multicast Address Range, page 62
- DEVICENAME Tag Not Supported for Directories Button, page 62


### Multicast Address Range

The Internal URI Features chapter of the *Cisco Unified IP Phone Services Application Development Notes* does not provide guidance on how to select a multicast address. For information on selecting a Multicast IP Address, see the Cisco Unified Communications System SRND, the IANA guidelines, and your local network administration policies.

### DEVICENAME Tag Not Supported for Directories Button

The IP Phone Service Configuration Settings table in the IP Phone Service Administration and Subscription of *Cisco Unified IP Phone Services Applicaton Development Notes* says that you can embed a special #DEVICENAME# substitution tag within a service URL. This tag works for either the Services or Messages buttons, but for the Directories button, the tag does not work on many older Cisco Unified IP phones.

## Disaster Recovery Administration Guide

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


- Managing Backup Devices, page 63
- Running Backups or Restores, page 63

- Alternative SFTP Servers, page 63
- DNS Information During Restore, page 63
- FAC and CMC Code is not Captured in CDR, page 65


## 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 servers in the cluster are running the same version of Cisco Unified Communications Manager. If different nodes 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.

# 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.

# Cisco Unified Communications Manager Features and Services Guide

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.

# Cisco Unified Communications Manager Call Detail Records Administration Guide

## Missing Redirect Reason Code

The following entry is missing from the “Redirect Reason Codes” table in the Cisco Unified Communications Manager Call Detail Records Administration Guide:

***Table 5 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 6 CDR Fields Order Corrections*

| Order in Document | Corrected Order |
|---|---|
| callIdentifier | directoryNumber |
| directoryNumber | callIdentifier |

*Table 7 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 |
| authorizationCode | | 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.

# Cisco Unified Real-Time Monitoring Tool Guide

## 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:<br>Log Partition Used Disk Space Exceeds Low Water Mark (90%) |

# Cisco Unified Communications Manager Security Guide

The following change exists for the Cisco Unified Communications Manager Security Guide:


- CSCuo97956 Unified CM8.5 documentation doesn't mention unrestricted VPN support, page 68
- Incorrect Configuration Example for ASA Router, page 68


## CSCuo97956 Unified CM8.5 documentation doesn't mention unrestricted VPN support

The "Virtual Private Network Setup" chapter of the Cisco Unified Communications Manager Security Guide omits the following information:

The U.S. export unrestricted version of Cisco Unified Communications Manager Release 8.5(1) does not support phone Virtual Private Networks (VPN).

## 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**

# 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.

# Cisco Unified Communications Manager Online Help

## Incorrect Description for Destination Number

This documentation update resolves CSCux74230.

The **Remote Destination Configuration Settings** field description in the Cisco Unified CM Administration Online Help incorrectly states that you can “Enter the telephone number for the destination”. The correct statement is “Enter the PSTN telephone number for the destination”.

## 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.

# 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)