Release Notes for Cisco Unified Communications Manager Release 7.1(5)

Updated May 25, 2010

Table 1 Updates to Release Notes for Cisco Unified Communications Manager Release 7.1(5)

Date	Update
May 25, 2010	Under Documentation Updates, added the "IP Phones That Work With Mobile Connect and Mobile Voice Access" section on page 75
May 24, 2010	Under Documentation Updates, added the "Updates to the Configuration Checklist for Cisco Extension Mobility" section on page 75
May 23, 2010	Under Important Notes, added the "Verify IPv6 Networking on Servers Before Upgrade" section on page 15
May 23, 2010	Under Documentation Updates, added the "Interaction of Single Number Reach and Privacy" section on page 76, "User Hold and Network Hold MOH Audio Source ID Cannot Be Defined Under Device Pool" section on page 76, and the "Enabling AAR for Hunt Pilots" section on page 65
May 21, 2010	Under Important Notes, added the "CSCte67180 Wrong Frequency Parameters in Database After an Upgrade Causes Failure" section on page 15
May 21, 2010	Under Documentation Updates, added the "Description of the Reset Button" section on page 65
May 7, 2010	Under Documentation Updates, added the "Circular Algorithm Description Is Incorrect" section on page 65

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

This document contains information that pertains to Cisco Unified Communications Manager (Cisco Unified CM) Release 7.1(5).

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

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.

Contents

This document includes the following topics:

Before you install or upgrade Cisco Unified Communications Manager (Cisco Unified CM), Cisco Systems recommends that you review the "Upgrading to Cisco Unified Communications Manager 7.1(5)" section on page 4 and the "Service Updates" section on page 13 for information pertinent to installing or upgrading, and the "Important Notes" section on page 14 for information about issues that may affect your system.

Note To ensure continuous operation and optimal performance of your Cisco Unified Communications Manager system, you should upgrade to Cisco Unified Communications Manager 7.1(5).

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.

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) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS 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 7.1(5).

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 7.1(5). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the *Cisco Unified Communications Manager Software Compatibility Matrix*. Cisco Unified CM requires a minimum of 2 GB of memory, 72 GB disk drive, and 2 GHz processor.

Uninterruptible Power Supply

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 You must connect MCS-7816 and MCS-7825 servers to a UPS to prevent file system corruption during power outages.

When Cisco Unified Communications Manager runs on one of the servers that are listed in Table 2, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported.

Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get 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 gets 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 commences as soon as the low battery threshold is reached. Resumption or fluctuation of power does 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.

Table 2 Supported Servers for Basic Integration

HP Servers	IBM Servers
MCS-7816-H3	MCS-7815-I1
MCS-7825-H1	MCS-7815-I2
MCS-7825-H2	MCS-7816-I3

Table 2 Supported Servers for Basic Integration (continued)

HP Servers	IBM Servers
MCS-7825-H3	MCS-7816-I3
MCS-7825-H4	MCS-7825-I1
MCS-7828-H3	MCS-7825-I2
MCS-7828-H4	MCS-7825-I3
MCS-7835-H2	MCS-7825I-30
MCS-7845-H2	MCS-7825-I4
MCS-7835-H3	MCS-7828-I3
MCS-7845-H3	MCS-7828-I4
	MCS-7828-I4
	MCS-7835-I1
	MCS-7835I-30
	MCS-7845-I2
	MCS-7835-I3
	MCS-7845-I3

Upgrading to Cisco Unified Communications Manager 7.1(5)

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

Before You Begin

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

   To do so, 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 5.

Special Upgrade Information

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

Upgrading to Unrestricted Cisco Unified Communications Manager Release 7.1(5)

Before you upgrade from Cisco Unified Communications Manager 6.x or 7.x to unrestricted Cisco Unified Communications Manager 7.1(5), install the unrestricted COP file that you can find here (copy and paste):

http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=282421166&sftType=Unified+Communications+Manager+Updates&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+7.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N

I/O Throttling

The Disable I/O Throttling check box was introduced in the Cisco Unified CM 7.1(2) upgrade window. Do not check this box. It is no longer required when upgrading to this release.

Write-Cache

A disabled write-cache on the server also causes the upgrade process to run more slowly. Multiple factors, including dead batteries on older servers, can cause the write-cache to get disabled.

Before starting an upgrade, verify the status of the write-cache on the MCS-7828-H4 and MCS-7835/45 disk controllers. You do not need to verify the write-cache status on the MCS-7816, MCS-7825, or on other MCS-7828 servers. To verify write-cache status, access Cisco Unified Operating System Administration, and choose **Show > Hardware**.

If you determine that your write-cache is disabled because of a dead battery, you need to replace the hard disk controller cache battery. Follow your local support procedures to get this battery replaced.

See the following examples of output from the **Show > Hardware** menu for details on determining the battery and write-back cache status.

The following example shows write-cache enabled. The example indicates that 50 percent of the cache is reserved for write and 50 percent of the cache is reserved for read. If the write-cache were disabled, 100 percent of the cache would be reserved for read or the Cache Status would not equal “OK.” Also, the battery count equals “1.” If the controller battery were dead or missing, the Battery Pack Count would indicate “0.”

Example 1 7835/45-H1, 7835/45-H2, 7828-H4 Servers with Write-Cache Enabled

---

```
RAID Details      :

Smart Array 6i in Slot 0
   Bus Interface: PCI
   Slot: 0
   Cache Serial Number: P75B20C9SR642P
   RAID 6 (ADG) Status: Disabled
   Controller Status: OK
   Chassis Slot:
   Hardware Revision: Rev B
   Firmware Version: 2.80
   Rebuild Priority: Low
   Expand Priority: Low
   Surface Scan Delay: 15 sec
   Cache Board Present: True
   Cache Status: OK
   Accelerator Ratio: 50% Read / 50% Write
   Total Cache Size: 192 MB
   Battery Pack Count: 1
   Battery Status: OK
   SATA NCQ Supported: False
```

The following example indicates that the battery status is enabled and that the the write-cache mode is enabled in (write-back) mode.

Example 2 7835/45-I2 Servers with Write-Cache Enabled

```
----------
RAID Details      :
Controllers found: 1

------------------------------------------------------------------------
Controller information
------------------------------------------------------------------------
   Controller Status                    : Okay
   Channel description                  : SAS/SATA
   Controller Model                     : IBM ServeRAID 8k
   Controller Serial Number             : 20ee0001
   Physical Slot                        : 0
   Copyback                             : Disabled
   Data scrubbing                       : Enabled
   Defunct disk drive count             : 0
   Logical drives/Offline/Critical      : 2/0/0
   ------------------------------------------------
   Controller Version Information
   ------------------------------------------------
   BIOS                                 : 5.2-0 (15421)
   Firmware                             : 5.2-0 (15421)
   Driver                               : 1.1-5 (2412)
   Boot Flash                           : 5.1-0 (15421)
   ------------------------------------------------
   Controller Battery Information
   ------------------------------------------------
   Status                               : Okay
   Over temperature                     : No
   Capacity remaining                   : 100 percent
   Time remaining (at current draw)     : 4 days, 18 hours, 40 minutes
   ------------------------------------------------
   Controller Vital Product Data
   ------------------------------------------------
   VPD Assigned#                        : 25R8075
   EC Version#                          : J85096
```

```
   Controller FRU#                     : 25R8076
   Battery FRU#                        : 25R8088

------------------------------------------------------------------------
Logical drive information
------------------------------------------------------------------------
Logical drive number 1
   Logical drive name                  : Logical Drive 1
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,0 0,1
Logical drive number 2
   Logical drive name                  : Logical Drive 2
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,2 0,3
```

Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(5) Upgrade

Before you upgrade to Cisco Unified Communications Manager 7.1(5), 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 Manager 7.1(5) 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.

Making Configuration Changes During an Upgrade

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

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

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

Upgrade Tasks

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

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

Procedure

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

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 over the first node to the upgraded partition.

Step 5 Switch over subsequent nodes to the upgraded partition.

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

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

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

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

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

Upgrade Paths to Cisco Unified Communications Manager 7.1(5)

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

Ordering the Upgrade Media

To upgrade to Cisco Unified CM Release 7.1(5), use the Product Upgrade Tool (PUT) to obtain a media kit and license or to 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 from Cisco Unified Communications Manager Release 5.1(3e) to 7.1(x) Releases

This information applies when you upgrade from any of the following releases to any 7.1.x release:

- 5.1(3e) (5.1.3.6000-2)
- The following 5.1(3e) Engineering Special releases:
  - 5.1(3.6103-1)
  - 5.1(3.6102-1)
  - 5.1(3.6101-1)

Before you upgrade, you must install the COP file ciscocm.513e_upgrade.cop.sgn on the server. Find this COP file at the following URL:

http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=COP-Files&mdfid=280735907&sftType=Unified+Communications+Manager%2FCallManager+Utilities&optPlat=&nodecount=2&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+5.1&treeMdfId

For information about installing this COP file, follow the installation instructions that are included with the COP file.

Note During an upgrade from a compatible Cisco Unified CM 5.1 version (see the Compatibility Matrix at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html) to Cisco Unified CM 7.1(5) by using a DVD, in the Software Installation/Upgrade window, ignore the checksum step that tells you "To ensure the integrity of the installation file, verify the MD5 hash value against the Cisco Systems website." Click "Next."

Upgrading to Unified CM 7.1(5) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_7.1.5.10000-12.sgn.iso, comprises two parts:

- UCSInstall_UCOS_7.1.5.10000-12.sgn.iso_part1of2
- UCSInstall_UCOS_7.1.5.10000-12.sgn.iso_part2of2

Procedure

Step 1 From the Software Download page on Cisco.com, download the two UCSInstall files.

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

Note Because the UCSInstall_UCOS_7.1.5.10000-12 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_7.1.5.10000-12.sgn.iso_part1of2 UCSInstall_UCOS_7.1.5.10000-12.sgn.iso_part2of2 > UCSInstall_UCOS_7.1.5.10000-12.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_7.1.5.10000-12.sgn.iso_part1of2+UCSInstall_UCOS_7.1.5.10000-12.sgn.iso_part2of2 UCSInstall_UCOS_7.1.5.10000-12.sgn.iso
```

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

64fa77e1ec9c9ede6f4066e36b631954 UCSInstall_UCOS_7.1.5.10000-12.sgn.iso

Step 4 Continue by following the instructions in the "Upgrading from a Local Source" section on page 10 or the "Upgrading from a Remote Source" section on page 11.

Upgrading from a Local Source

To upgrade the software from local DVD, use 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 Merely 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 disable throttling, check the **Disable I/O throttling** check box.

Caution Although disabling throttling decreases the time to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the "I/O Throttling" section on page 5.

If you want to reenable throttling after you start the upgrade, you must cancel the upgrade, reenable throttling, and then restart the upgrade.

Step 8 To continue the upgrade process, click **Next**.

Step 9 Choose the upgrade version that you want to install and click **Next**.

Step 10 In the next window, monitor the progress of the download.

Step 11 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and runs the upgraded software.

Step 12 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, perform the following steps:

a. Choose **Do not reboot after upgrade**.

b. Click **Next**.

The Upgrade Status window displays the Upgrade log.

c. When the installation completes, click **Finish**.

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

The system restarts and runs 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 the interface provides.

Procedure

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

If you are upgrading from a supported 5.1(x) release, the upgrade requires a set of files that is called a *patch set*. Put the patch set files on the FTP or SFTP server by using one of these methods:

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 that 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 disable throttling, check the **Disable I/O throttling** check box.

Caution Although disabling throttling decreases the time to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the "I/O Throttling" section on page 5.

If you want to reenable throttling after you start the upgrade, you must cancel the upgrade, reenable throttling, and then restart the upgrade.

Step 11 To continue the upgrade process, click **Next**.

Step 12 Choose the upgrade version that you want to install; then, click **Next**.

- If you are upgrading from Cisco Unified Communications Manager Release 5.1(x), the upgrade requires a set of files that is called a *patch set*. Choose the upgrade version to install from the list. The upgrade version name does not include any file extensions, because it represents a patch set.
- If you are upgrading from Cisco Unified Communications Manager Release 6.x or 7.x, the upgrade file has the extension sgn.iso.

Step 13 In the next window, monitor the progress of the download.

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

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

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

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

Step 14 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and runs the upgraded software.

Step 15 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, perform the following steps:

a. Choose **Do not reboot after upgrade**.

b. Click **Next**.

The Upgrade Status window displays the Upgrade log.

c. When the installation completes, click **Finish**.

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

The system restarts and runs the upgraded software.

Service Updates

After you install or upgrade to this release of Cisco Unified Communications Manager, check to see whether Cisco has released critical patches or Service Updates. Service Updates, or SUs, contain fixes that were unavailable at the time of the original release. SUs often include security fixes, firmware updates, or software fixes that can improve operation.

To check for updates, 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 Unified Communications Manager for your deployment*.

For continued notification of updates for your Cisco products, subscribe to the Cisco Notification Service at:

http://www.cisco.com/cisco/support/notifications.html

Related Documentation

The view documentation that supports Cisco Unified CM Release 7.1(5), go to http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.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 7.1(5) as part of Cisco Unified Communications System Release 7.1 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 CM Release 7.1(5). 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 7.1(5).

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.

CSCte67180 Wrong Frequency Parameters in Database After an Upgrade Causes Failure

Incorrect frequency configurations in the database, after an upgrade from Cisco Unified Communications Manager 6.x result in save failure of alert configurations from the user interface.

Workaround

Modify the alert configuration with valid frequency parameters and proceed with save configuration operation.

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

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

Conditions

Under rare critical failures, such as a kernel panic, the IBM I3-type servers do not automatically get restarted by the BIOS ASR functionality and logs the event. The server remains unresponsive until it is rebooted manually. In **IMM Control > System Settings > Server Timeouts**, the OS Watchdog timeout default specifies disabled.

Workaround

Manually set the OS Watchdog timer to the time interval during which the watchdog should check for activity.

Caution Currently the ASR / OS Watchdog feature gets triggered unexpectedly during fresh install and potentially during upgrade from 7.1(3) to 7.1(5). If the server is restarted due to Watchdog Timer expiring the install or upgrade may fail.

Until this defect gets resolved, use the ASR / OS Watchdog feature with care. Before a fresh install or upgrade, disable the OS Watchdog Feature by using IMM to avoid unexpected failures.

CSCtf15332 Node Licenses Missing After an Upgrade

If the node license file contains multiple features (for example: SW_FEATURE + CCM_NODE), after you upgrade to this release of Cisco Unified Communications Manager, the following licensing warnings might display:

- System is operating on insufficient licenses.
- Please upload additional license files.

For additional details and workaround, see CSCtf15332.

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.

CSCte56322 Netscape Browser is not Supported

The Netscape browser is no longer supported. Supported browsers comprise Internet Explorer (IE) 7 or 8, Firefox 3.x, or Safari 4.x.

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.

Unified CM 7.x IOS Device Does Not Offer Full NAT Support for SCCP Version 17

Caution Cisco recommends that you consider CSCsy93500 when you design a network that employs Network Address Translation (NAT) and Cisco Unified Communications Manager 7.x simultaneously.

At the time of Cisco Unified CM 7.x release, no IOS device offers full NAT support for the SCCP version that this release employs.

Status Updates

CSCsy93500 tracks the status of support for NAT in SCCP version 17. For updates, subscribe to updates in bug toolkit for CSCsy93500.

CSCtc99413 Upgrade to Unified CM 7.1(3x) from Unified CM 5.x Results in Low Active Partition Disk Alerts

When you upgrade from Cisco Unified Communications Manager Release 5.x to Cisco Unified Communications Manager 7.1(3)or later, low active partition disk alerts occur.

WorkAround

Perform the following steps:

Step 1 Lower the threshold for the low active partition disk space warning to less than 4%.

Step 2 Back up your system.

Step 3 Perform a fresh installation.

Step 4 Restore the system so that the disk gets repartitioned and is no longer limited by the inefficient 5.x disk partitioning.

Disaster Recovery System Caution

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

CSCso98836 HP Ultra320 SCSI HDD FW Upgrade

A ProLiant server that is configured with any of the HP Ultra320 SCSI hard drives that are listed in HP Customer Advisory **#C00859596** (available at http://www.hp.com) may exhibit timeouts and SCSI downshifts.

These problems may occur on the following server models:

- MCS-7835-1266 (DL380-G2)
- MCS-7835H-2.4 (DL380-G3)
- MCS-7835H-3.0 (DL380-G3)
- MCS-7835-H1 (DL380-G4)
- MCS-7845-1400 (DL380-G2)
- MCS-7845H-2.4 (DL380-G3)
- MCS-7845H-3.0 (DL380-G3)
- MCS-7845-H1 (DL380-G4)

The associated HP Customer Advisories list the affected hard drives that experience these problems. However, you can apply the Cisco-provided HP SCSI Hard Drive Firmware Update CD to all listed server types and the impacted drives get updated if applicable.

To update the firmware to a Cisco-tested level, use the Cisco provided HP SCSI Hard Drive Firmware Update CD released simultaneous to the Unified Communications 7.0(1) system release. For more details on installing the firmware, see the README.txt file for HP SCSI Hard Drive Firmware Update CD.

You can obtain the ISO image for the Cisco-provided HP SCSI Hard Drive Firmware Update CD and associated readme file from Cisco.com at the following navigation path:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

From the Tools & Resources Download Software page, go to:

Communications Infrastructure >

Voice Servers >

Cisco 7800 Series Media Convergence Servers >

<SERVER MODEL>

Latest Releases >

Firmware >

<Select: HP_SCSI_FW-1.0.1.iso>

<Select: HP_SCSI_FW-Readme.txt>

CSCtb95488 Phones That Support Monitoring and Recording Features

The "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide, Release 7.1(2),* includes a partial list of devices that support monitoring and recording in the "Agent Devices" subsection of the "Devices That Support Call Monitoring and Call Recording" section.

The list of devices that support the monitoring and recording features varies per version and device pack.

Use the Cisco Unified Reporting application to generate a complete list of devices that support monitoring and recording for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File > Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.
4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.
5. To generate a report of all devices that support monitoring, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Monitor

   The List Features pane displays a list of all devices that support the monitoring feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

6. To generate a report of all devices that support recording, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Record

   The List Features pane displays a list of all devices that support the recording feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

For additional information about the Cisco Unified Reporting application, refer to the *Cisco Unified Reporting Administration Guide*, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

LogCollectionPort Service: selectLogFiles Operation

Description

The selectLogFiles operation retrieves log files based on a selection criteria. This API takes FileSelectionCriteria object as an input parameter and returns the file name and location for that object.

The LogCollectionService URL specifies
http://hostname/logcollectionservice/services/LogCollectionPort

Parameters

The selectLogFiles operation includes the following elements:

- ServiceLogs—Array of strings. The available service options depends on the services that are activated on the Cisco Unified CM. The actual available options are those that the listNodeServiceLogs operation returns at run time. For example:
  - Cisco Syslog Agent
  - Cisco Unified CM SNMP Service
  - Cisco CDP Agent
- SystemLogs—Array of strings.

Note SystemLogs element is not available in Cisco Unified CM release 7.1.3, and therefore should be empty.

- JobType—The collection type. The available options are the following:
  - DownloadtoClient
  - PushtoSFTPServer

  If you select PushtoSFTPServer, the following elements are also required:
  - IPAddress
  - UserName
  - Password
  - Port
  - Remote Download Folder
- SearchStr—A non-null string.
- Frequency—The frequency of log collection. The available options are the following:
  - OnDemand
  - Daily
  - Weekly
  - Monthly

Note Only OnDemand option is currently supported for the Frequency element. The other options (Daily, Weekly, and Monthly) apply to schedule collection, which is currently not supported.

- ToDate—The end date for file collection. Format is **mm/yy/dd hh:mm AM/PM.** The ToDate element is required if you use absolute time range.
  File collection time range can be absolute or relative. If you prefer relative time range, the following elements are required:
  - RelText
  - RelTime

  If you prefer absolute time range, then the following elements are required:
  - ToDate
  - FromDate
- FromDate—The start date for file collection. Format is **mm/yy/dd hh:mm AM/PM.** The FromDate element is required if you use absolute time range.
- RelText—The file collection time range. The available options are:
  - Week
  - Day
  - Month
  - Hours
  - Minutes
- RelTime—The file collection time value. Gives all files from the specified time up to present. The available range specifies 1 to 100.
  For example, if the RelText is "Day" and RelTime is 1, then we get all files modified in the previous one day.
- TimeZone—The time zone value. The format is **Client: (GMT ±*n*) *Name of the time zone*** where n is the offset time of the specified time zone and GMT. For example:
  - Client: (GMT-0:0) Greenwich Mean Time
  - Client: (GMT-8:0) Pacific Standard Time
- Port—The port number of the node.
- IPAddress—The IP address of the node.
- UserName—The service administrator username for the node.
- Password—The service administrator password for the node.
- ZipInfo—Indicates whether to compress the files during collection. This element is applicable only for PushtoSFTPServer option. The available options are:
  - True—The files are compressed.
  - False—The files are not compressed.
- RemoteFolder—The remote folder where the files are to be uploaded. This option is used only if you choose to upload trace files to SFTP or FTP server.

Request Example

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
```

```
  <ns1:SelectLogFiles soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
   <FileSelectionCriteria href="#id0"/>
  </ns1:SelectLogFiles>
  <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:SchemaFileSelectionCriteria"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
   <ServiceLogs xsi:type="soapenc:Array" soapenc:arrayType="xsd:string[45]">
    <item>Cisco Syslog Agent</item>
    <item>Event Viewer-Application Log</item>
    <item>Install Logs</item>
    <item>Event Viewer-System Log</item>
    <item>Security Logs</item>
   </ServiceLogs>

   <SystemLogs xsi:type="xsd:string" xsi:nil="true"/>

   <JobType href="#id2"/>
   <SearchStr xsi:type="xsd:string"/>
   <Frequency href="#id1"/>
   <ToDate xsi:type="xsd:string" xsi:nil="true"/>
   <FromDate xsi:type="xsd:string" xsi:nil="true"/>
   <TimeZone xsi:type="xsd:string">Client:(GMT-8:0)Pacific Standard Time</TimeZone>
   <RelText href="#id3"/>
   <RelTime xsi:type="xsd:byte">5</RelTime>
   <Port xsi:type="xsd:byte">0</Port>
   <IPAddress xsi:type="xsd:string">MCS-SD4</IPAddress>
   <UserName xsi:type="xsd:string" xsi:nil="true"/>
   <Password xsi:type="xsd:string" xsi:nil="true"/>
   <ZipInfo xsi:type="xsd:boolean">false</ZipInfo>
  </multiRef>
    <multiRef id="id1" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns4:Frequency"
xmlns:ns4="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">OnDemand</multiRef>
    <multiRef id="id2" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns3:JobType"
xmlns:ns3="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">DownloadtoClient</multiRef>
    <multiRef id="id3" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns4:RelText"
xmlns:ns4="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">Hours</multiRef>
 </soapenv:Body>
</soapenv:Envelope>
```

Response Example

The response returns a FileSelectionResult object, which contains the list of matching file names and their location in the server.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:SelectLogFilesResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
<FileSelectionResult xsi:type="ns2:SchemaFileSelectionResult"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
```

```
<Node xsi:type="ns2:Node">
<name xsi:type="xsd:string">MCS-SD4</name>
<ServiceList soapenc:arrayType="ns2:ServiceLogs[1]" xsi:type="soapenc:Array"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<item xsi:type="ns2:ServiceLogs">
<name xsi:type="xsd:string" xsi:nil="true"/>
<SetOfFiles soapenc:arrayType="ns2:file[5]" xsi:type="soapenc:Array">
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000305.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000305.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097082</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 04:14:05 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000306.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000306.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097083</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 05:41:26 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000307.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000307.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096868</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 07:08:56 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000308.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000308.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096838</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:36:17 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000309.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000309.txt</absolu
tepath>
<filesize xsi:type="xsd:string">100657</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:40:20 PST 2009</modifiedDate>
</item>
</SetOfFiles>
</item>
</ServiceList>
</Node>
</FileSelectionResult>
<ScheduleList soapenc:arrayType="ns3:Schedule[0]" xsi:type="soapenc:Array"
xmlns:ns3="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"/>
</ns1:SelectLogFilesResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Fault

If the specified frequency is null, it throws a remote exception, “LogCollection frequency is null.” If the array of ServiceLogs and System Logs is null, it throws a remote exception, “No Service/Syslog are provided for the collection.” If a matching file is not found, it throws a remote exception, “The File Vector from the server is null.”

Perform DRS Backup After You Regenerate Certificates

After you regenerate certificates in Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificate(s). 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 on performing a backup, refer to the *Disaster Recovery System Administration Guide*.

Important Information About Create File Format Capability in BAT

The Create File Format window provides the option to set the maximum number of Lines, Speed Dials, and so on. The file format that gets created by using BAT stores the selected Device, Line, Intercom, Speed Dial, BLF Speed Dial, BLF Directed Call Park, and IP Phone Service fields in the database. Because the database column length allows up to 32K characters, the BAT Administrator cannot choose all the fields with maximum allowed number because this will exceed 32K. When the file format length exceeds 32K, BAT displays the following error message:

“Cannot Insert a file format with characters more than 32K"

The BAT Administrator must use BAT Phone Templates to define the common attributes.

Limitation Between QSIG PRI and SIP Trunk for MWI

In previous releases of Cisco Unified CM, to route an MWI request from QSIG PRI to a SIP trunk, the route pattern that was specified had to point directly to the SIP trunk.

If the route pattern pointed to a Route List/Route Group that included the SIP trunk, MWI failed. After the first failure, all subsequent MWI indications to any number in the cluster failed.

In Cisco Unified CM 7.x, the MWI routing gets handled differently.

If MessageWaiting gets an SsDataInd signal while in the mwi_nailed_up_ssinfores state, MessageWaiting does not process any subsequent MWIs.

SDL traces should look like the example below, which indicates that a previous MWI request caused the system to hit the limitation.

```
2009/07/15 23:36:15.902| 002| SdlSig    | SsDataInd                              |
mwi_nailed_up_ssinfores       | MessageWaiting(2,100,126,4352)  |
MessageWaitingManager(2,100,125,1)| (2,100,124,1).15384643-(*:10.40.30.12)  | [R:NP -
HP: 0, NP: 0, LP: 0, VLP: 0, LZP: 0 DBP: 0]SsType=33554444 SsKey=0 SsNode=2
SsParty=39330436 DevId=(0,0,0) BCC=9 OtherParty=39330437 NodeOtherParty=2 clearType =
0 CSS=169e2389-5c0b-4500-88e7-2cb6244fd8b1 CNumInfo = 0 CNameInfo = 0 ssDevType=6
ssOtherDevType=5FDataType=1opId=81invokeId=-29584resultExp=0 fac.fid=28 fac.l=32
fac.fid=28 fac.l=1 fac.fid=28 fac.l=1 ssCause = 0 ssUserState = 2 ssOtherUserState = 1
```

Cisco Unified Communications Manager Assistant Wizard Constraint

Be aware that you can run the IPMA Wizard only once. Attempts to run it more than once will fail.

Creating a Custom Help Desk Role and Custom Help Desk User Group

Some companies want their help desk personnel to have privileges to be able to perform certain tasks, such as adding a phone, adding an end user, or adding an end user to a user group in Cisco Unified Communications Manager Administration.

Performing the steps in the following example allows help desk personnel to add a phone, add an end user, and add the end user to the Standard CCM End Users user group, which allows an end user to access and update the Cisco Unified CM User Options.

Example—Allows Help Desk Personnel to Add Phone, Add End User, and Add End User to User Group

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management > Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list box, choose **Cisco Unified CM Administration**; then, click **Next**.

Step 4 In the Name field, enter the name of the role; for example, Help Desk.

Step 5 In the Description field, enter a short description; for example, for adding phones and users.

Step 6 Choose one of the following options, which depends on where you want the help desk personnel to perform the task:

a. If you want the help desk personnel to add a phone in the Phone Configuration window and then add an end user in the End User Configuration window. check the **read** and **update** privileges check boxes for the User web page resource and the Phone web pages resource; then, click **Save**.

b. If you want the help desk personnel to add both a phone and a user at the same time in the User and Phone Add window, check the **read** and **update** privileges check boxes for the User and Phone add resource and the User web page resource; then, click **Save**.

Step 7 By performing the following tasks, you create a custom user group for the help desk:

a. In Cisco Unified Communications Manager Administration, choose **User Management > User Group**; then, click **Add New**.

b. Enter the name of the custom user group; for example, Help Desk.

c. From the Related Links drop-down list box, choose **Assign Roles to User Group**; then, click **Go**.

d. Click the **Assign Role to Group** button.

e. Check the check box for the custom role that you created in Step 1 through Step 6; in this example, Help Desk. In addition, check the check box for the Standard CCM Admin Users role; then, click **Add Selected**.

f. In the User Group Configuration window, verify that the roles display in the Role Assignment pane; then, click **Save**.

Next Steps

In Cisco Unified Communications Manager Administration, the help desk personnel can add the phone, add the user, and add the end user to the user group.

- To add a phone in the Phone Configuration window, choose **Device > Phone**; then, to add an end user in the End User window, choose **User Management > End User**.
- To add both a phone and user at the same time in the User and Phone Add window, choose **User Management > User and Phone Add**.
- To associate the end user with the Standard CCM End Users user group, choose **User Management > User Group**.

Tip For more information on how to perform these tasks in Cisco Unified Communications Manager Administration, refer to the *Cisco Unified Communications Manager Administration Guide*.

Do Not Unplug a USB Device While It Is In Use

Do not unplug a USB device that is in use from the Cisco Unified Communications Manager server. If you do, the USB device will become inaccessible, and messages will display on the server console.

Removing Hard Drives

Cisco only supports replacing failed hard drives. Cisco does not support drive pulling/swapping as a method of fast upgrade reversion, restore, or server recovery. For information on replacing a failed hard drive, refer to the *Troubleshooting Guide for Cisco Unified Communications Manager*.

CSCsx96370 Multiple Tenant MWI Modes Service Parameter

The Multiple Tenant MWI Modes service parameter, which supports the Cisco CallManager service, specifies whether to apply translation patterns to voice-message mailbox numbers. Valid values specify True, which means that Cisco Unified Communications Manager uses translation patterns to convert voice-message mailbox numbers into directory numbers when your voice-messaging system issues a command to set a message waiting indicator; or False, which means that Cisco Unified Communications Manager does not translate the voice-message mailbox numbers that it receives from your voice-messaging system.

Be aware that this service parameter supports Cisco Unified Communications Manager integrations with Cisco Unity Connection or Cisco Unity. If your voice-mail extensions require translation in Cisco Unified Communications Manager, set the Multiple Tenant MWI Modes service parameter to **True** after you install or upgrade to Cisco Unified Communications Manager 7.1(5).

Considerations for LDAP Port Configuration

When you configure the LDAP Port field in Cisco Unified Communications Manager Administration, you specify the port number that the corporate directory uses to receive LDAP requests. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers.

Your configuration may require that you enter a different port number than the numbers that are listed in the following items. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

LDAP Port for When the LDAP Server Is Not a Global Catalog Server

- 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

LDAP Port for When the LDAP Server Is a Global Catalog Server

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Configuring the Hostname/IP Address for the Cisco Unified Communications Manager Server

Table 3 lists the locations where you can configure a host name for the Cisco Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Cisco Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Caution Before you change the host name or IP address for any locations that are listed in Table 3, refer to *Changing the IP Address and Host Name for Cisco Unified Communications Manager 7.1(2)*. Failing to update the host name or IP address correctly after it is configured may cause problems for Cisco Unified Communications Manager.

Table 3 Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System > Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for any server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation	You can add the host name for any server in the cluster.	1-63	alphabetic	alphanumeric

Table 3 Host Name Configuration in Cisco Unified Communications Manager (continued)

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Hostname field **Settings > IP > Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric
set network hostname *hostname* Command Line Interface	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location in Table 3, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  After you install Cisco Unified Communications Manager on the publisher database server, the host name for the publisher automatically displays in this field. Before you install Cisco Unified Communications Manager on the subscriber server, enter either the IP address or the host name for the subscriber server in this field on the publisher database server.

  In this field, only configure a host name if Cisco Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

  Tip In addition to configuring Cisco Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the Cisco Unified Communications Manager installation of the publisher database server, you enter the host name, which is mandatory, and IP address of the publisher server to configure network information; that is, if you want to use static networking.

  During the Cisco Unified Communications Manager installation on the subscriber server, you enter the hostname and IP address of the publisher database server, so Cisco Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber server. When the Cisco Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

Related Topics

- "Server Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*

- *Installing Cisco Unified Communications Manager, Release 7.1(2)*
- *Cisco Unified Communications Operating System Administration Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions Release 7.1(3-22)*
- *Changing the IP Address and Host Name for Cisco Unified Communications Manager 7.1(2)*

SFTP Server Products

Cisco allows you to use any SFTP server product with applications that require SFTP access but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://www.cisco.com/pcgi-bin/ctdp/Search.pl. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx. Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

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

Cisco does not support freeFTDP because of the 1 GB file size limit on this SFTP product.

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

Important Information About Delete Transaction by Using Custom File in BAT

Do not use the insert or export transaction files that are created with bat.xlt for the delete transaction. Instead, you must create a custom file with the details of the records that need to be deleted. Use only this file for the delete transaction. In this custom delete file, you do not need a header, and you can enter values for name, description, or user.

TAPS Name Change in Bulk Administration Tool

Documentation refers to the Tool for Auto-Registered Phone Support (TAPS) as Cisco Unified Communications Manager Auto-Register Phone Tool in the Online Help for Bulk Administration. All references to “Cisco Unified Communications Manager Auto-Register Phone Tool” in the Bulk Administration Tool Online Help should be read as 'Tool for Auto-Registered Phone Support (TAPS)'. This makes the terminology compliant with the Bulk Administration user interface.

For More Information

For information on configuring additional features in Bulk Administration Tool, refer to the BAT documentation for Cisco Unified CM.

Basic Uninterruptible Power Supply (UPS) Integration

When Cisco Unified Communications Manager runs on an MCS 7825H2 or MCS 7835H2, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported. Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, on MCS-7835H2, you can execute the **show ups** CLI command that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started.

On supported servers, 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 starts as soon as the low battery threshold is reached. Resumption or fluctuation of power does not interrupt or abort the shutdown.

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.

Strict Version Checking

Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.

Note Make sure that the restore runs on the same Cisco Unified Communications Manager version as the backup. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore.

Consider the following examples of restore to understand strict version checking:

Table 4 Restore Examples

From version	To version	Allowed / Not allowed
7.1(3).1000-1	7.1(5).1000-1	Not allowed
7.1(5).1000-1	7.1(5).1000-2	Not allowed
7.1(5).1000-1	7.1(5).2000-1	Not allowed
7.1(5).1000-1	7.1(5).1000-1	Allowed

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.

Serviceability Not Always Accessible from OS Administration

In some scenarios, you cannot access Cisco Unified Serviceability from Cisco Unified OS Administration. The window displays a "Loading, please wait" message indefinitely.

If the redirect fails, log out of Cisco Unified OS Administration, select Cisco Unified Serviceability from the navigation menu, and log in to Cisco Unified Serviceability.

Voice Mailbox Mask Interacts with Diversion Header

When a call gets redirected from a DN to a voice-messaging server/service that is integrated with Unified CM by using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. Be aware that this behavior is expected because the Unified CM server uses the diversion header to choose a mailbox.

Best Practices for Assigning Roles to Serviceability Administrators

Cisco recommends that you configure application users, rather than end users, to access remote nodes to perform such tasks as starting and stopping services. Starting and stopping services requires that the Standard Serviceability Administration and Standard RealtimeAndTraceCollection roles be assigned.

For Serviceability, the Administrator That Is Created During Installation Must Not Be Removed

Removing the Administrator that is created during installation or upgrade can cause communication with remote nodes via Serviceability Administration to fail.

Connecting to Third-Party Voice Messaging Systems

Administrators can connect third-party voice-messaging systems to Cisco Unified Communications Manager. Ensure that the voice-messaging system has a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager Release 5.0 or later, use a Cisco-certified serial-to-USB adapter with the part number USB-SERIAL-CA=.

Database Replication When You Revert to an Older Product Release

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

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message that reminds you about the requirement to reset database replication if you are reverting to an older product release. The caveats CSCsl57629 and CSCsl57655 also document this behavior.

For information about the **utils dbreplication clusterreset**, **utils dbreplication dropadmindb**, and **utils dbreplication forcedatasyncsub** commands, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions Release 7.1(3)* document at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/7_1_3/cli_ref_713.html.

User Account Control Pop-up Window Displays During Installation of RTMT

When you install RTMT on the Microsoft Vista platform, the system displays the User Account Control pop-up window to indicate that an unidentified program wants access to your computer. This occurs because of a limitation in the InstallAnywhere software. This one-time pop-up displays only when you are installing RTMT. To continue, select **Allow**.

CiscoTSP Limitations on Windows Vista Platform

Always perform the first-time installation of the CiscoTSP and Cisco Unified Communications Manager TSP Wave Driver on a Vista machine as a fresh install.

If secure connection to Cisco Unified Communications Manager is to be used, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for inbound audio streaming, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for audio streaming, disable all other devices in the “Sound, video and game controllers” group.

Time Required for Disk Mirroring

Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately three hours.

Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately four hours.

Changes to Cisco Extension Mobility After Upgrade

If you chose a user-created profile from the Log Out Profile drop-down list on the Phone Configuration window and checked the **Enable Extension Mobility** check box, the settings in that profile become the permanent settings on the phone after an upgrade from Cisco Unified CallManager 4.x or Cisco Unified Communications Manager 5.x to Cisco Unified Communications Manager 6.1(1a).

RTMT Requirement When Cisco Unified Communications Manager Is Upgraded

If you run the Cisco Unified Communications Real Time Monitoring Tool (RTMT) client and monitor performance counters during a Cisco Unified Communications Manager upgrade, the performance counters do not update during and after the upgrade. To continue monitoring performance counters accurately after the upgrade completes, you must either reload the RTMT profile or restart the RTMT client.

Serviceability Session Timeout Is Not Graceful

When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before it indicates that the session timed out and redirects you to the login window. After you log in again, you may need to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows.

Workaround

If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before you make any changes in the user interface.

Serviceability Limitations When You Modify the IP Address

When you modify the IP Address field, you cannot access the RTMT profiles, custom counters, custom alerts, and generic queries for Trace and Log Collection Tool (TLC) for that server.

You should manually remove any RTMT profiles, custom counters, custom alerts, and generic queries for Trace and Log Collection Tool (TLC) that were set for the old IP Address. If you modify the IP Address field, you will need to re-create the RTMT profile, custom counters, custom alerts, and generic queries for TLC the next time that you log in to the server on RTMT.

Cisco AMC Service includes two user-configurable service parameters, Primary Collector and Failover Collector. These service parameters use Host Name/IP Address to designate the primary and failover AMC server. If you change the IP address of the AMC primary collector or failover collector, you should check these service parameters and update them accordingly.

Cisco Serviceability Reporter service includes one user-configurable service parameter, RTMT Reporter Designated Node. This service parameter uses Host Name/IP Address to designate the node on which RTMTReporter runs. If you changed the IP address of the RTMT Reporter Designated Node, you should check this service parameter and update it accordingly.

New and Changed Information

Note For New and Changed Information for earlier releases in the 7.x release train, see the release notes at http://www.cisco.com/en/US/products/sw/voicers/ps556/prod_release_notes_list.html.

This section contains information on new or updated features specific to Cisco Unified Communications Manager 7.1(5).

Command Line Interface

This section contains updates and additions that appear in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions, Release 7.1(5).*

Commands Added

The following commands got added to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions, Release 7.1(5).*

- utils ldap config fqdn, page 34
- utils ldap config ipaddr, page 34

utils ldap config fqdn

This command configures the system to use an FQDN for LDAP authentication, which is the preferred method.

Note Because this method requires that DNS be configured, if the system is not configured to use DNS, execute **utils ldap config ipaddr** instead.

Command Syntax

utils ldap config fqdn

Requirements

Command privilege level: 0

Allowed during upgrade: No

utils ldap config ipaddr

This command configures the system to use an IP address for LDAP authentication.

Note Because using an IP address for LDAP authentication is not the preferred method, use this command if the system is not, or cannot, be configured to use DNS. If your system is configured to use DNS, use **utils ldap config fqdn** instead.

Command Syntax

utils ldap config ipaddr

Requirements

Command privilege level: 0

Allowed during upgrade: No

Command Updated

The following command got updated in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions, Release 7.1(5)*:

- set network domain, page 35

set network domain

This command sets the domain name for the system.

Command Syntax

set network domain *domain-name*

Parameters

- *domain-name* represents the domain in which the system resides.

Usage Guidelines

The system asks whether you want to continue to execute this command.

Caution If you continue, this command causes a temporary loss of network connectivity.

The domain name must follow the rules for ARPANET host names, which specify the following:

- Must start with a letter.
- Must end with a letter or number.
- Must be 63 characters or less in length.
- Must be at least one character in length.
- May contain alphanumeric characters (A - Z, a - z, and 0 - 9) and hyphens (-).

Note Upper- and lowercase letters are allowed in domain names, but no significance is attached to the case. That is, two names with the same spelling but different case get treated identically.

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

- New and Updated Enterprise and System Parameters, page 35
- Menu Changes, page 36
- Cisco Unified Communications Manager Features and Applications, page 37

New and Updated Enterprise and System Parameters

The following sections contain information on new and updated enterprise and service parameters:

- Enterprise Parameters, page 36
- Service Parameters, page 36

Enterprise Parameters

No new or updated enterprise parameters exist in Cisco Unified Communications Manager 7.1(3x).

Service Parameters

To access the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**. Choose the server and the service name that the parameter supports. For some parameters, you may need to click Advanced to display the service parameter. To display the help for the service parameter, click the name of the service parameter in the window.

- Always Use Preferred G.729 Packet Size For SIP Trunk Answers

  This parameter determines whether the value specified in the Preferred G.729 Millisecond Packet Size service parameter is always used in outgoing answers that contain G.729 (including any of the four variants: G.729, G.729a, G.729b, or G.729ab) and that are sent to SIP Trunks. Valid values specify True or False; the default value specifies False.

  When set to True, the preferred G.729 packet size is used as the G.729 ptime (packetization time) in the outgoing answer to the SIP trunk only when Cisco Unified Communications Manager selects G.729 from the codecs in the offer, regardless of which G.729 ptime is specified in the incoming offer from the trunk. This answer to the SIP trunk tells the device behind the trunk to send a G.729 stream with that packet size to the other party in the call. The other party in the call also gets signaled to stream G.729 with that packet size to the device behind the SIP trunk. However, if the other party uses SCCP, H.323, or MGCP, and the preferred packet size exceeds the packet size that the other party advertises, the other party's advertised packet size gets used instead for both the outgoing answer to the SIP trunk and for the signals to the other party. This service parameter applies only to calls in which media resources (including media termination points and transcoders) are not allocated.

  When set to False, the preferred G.729 packet size gets used only when it does not exceed the packet sizes that the SIP trunk and the other party in the call advertise. This procedure is normally used for all audio codecs.

Menu Changes

This section contains information on the following menus in Cisco Unified Communications Manager Administration:

Main Window

No changes exist for the main window.

System

The System menu contains the following updates:

- System > Service Parameters—See the "New and Updated Enterprise and System Parameters" section on page 35.

Call Routing

No changes exist for the Call Routing menu.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

No changes exist for the Device menu.

Application

No updates or new fields exist for this menu.

User Management

No updates or new fields exist for this menu.

Bulk Administration

The Bulk Administration menu displays the following new and updated settings:

- Feature control policy settings display

Cisco Unified Communications Manager Features and Applications

This section contains information on the following Cisco Unified Communications Manager Administration features and applications:

Fujitsu Mobile Phone Support (SIP)

Two new third-party SIP phones are now supported in Cisco Unified Communications Manager: Fujitsu PHS Access Unit and Mobile Access Manager. These devices are supported through CTI to initiate calls and perform XSI DeviceDataPassThrough requests only.

The new devices are installed by using a Cisco Options Package (COP). In addition to the two devices, each phone has an associated phone template and security profile.

After the COP file is installed, configure the Fujitsu PHS and FOMA SIP devices in Cisco Unified Communications Manager Phone Configuration and Application User Configuration. After the devices are configured, Cisco Unified Communications Manager automatically allocates three device license units for each device.

Fujitsu Mobile Access Unit supports the Cisco Unified Mobility feature.

Use the following procedure to configure the Fujitsu PHS Access Unit.

Procedure

Step 1 Use Cisco Unified Communications Operating System Administration to install the COP file for the Fujitsu SIP devices.

Step 2 Choose **Software Upgrades > Install/Upgrade**.

The filename is cmterm-Fujitsu_PHS-1.2-6.1.cop.sgn.

Step 3 Use Cisco Unified Communications Manager Phone Configuration to add the Fujitsu PHS-AU device. (Auto Registration is not supported).

Step 4 Choose **Device > Phone**.

Step 5 Click **Add New**.

Step 6 Choose the Fujitsu PHS-AU device as the Phone Type.

Step 7 Enter the appropriate settings as defined in Table 5.

Step 8 Click **Save**.

Step 9 Use Cisco Unified Communications Manager Administration User Management to add an application user.

Step 10 Choose **User Management > Application User**.

Step 11 Click **Add New**.

Step 12 Enter the appropriate settings as defined in Table 6.

Step 13 Click **Save**.

Table 5 Fujitsu PHS Access Unit SIP Device Configuration Settings

Field	Description
MAC Address	For example, 400000002040
Device Pool	Default
Phone Button Template	FJ-Standard PHS-AU
Device Security Profile	Fujitsu PHS-AU Standard SIP Non-Secure Profile
SIP Profile	Standard SIP Profile

Table 6 Fujitsu PHS Access Unit SIP Application User Configuration Settings

Field	Description
User ID	For example, jtapiuser
Password	Enter a password of your choice.
Controlled Device	SEP400000002040
User Group	Standard CTI Enabled

Use the following procedure to configure the Fujitsu Mobile Access Manager.

Procedure

Step 1 Use Cisco Unified Communications Operating System Administration to install the COP file for the Fujitsu SIP devices.

Step 2 Choose **Software Upgrades > Install/Upgrade**.

The filename is cmterm-Fujitsu_MBL-AU(D)-1.1-6.1.cop.sgn.

Step 3 Use Cisco Unified Communications Manager Phone Configuration to add the Fujitsu MBL-AU device. (Auto Registration is not supported).

Step 4 Choose **Device > Phone**.

Step 5 Click **Add New**.

Step 6 Choose the Fujitsu MBL-AU device as the Phone Type.

Step 7 Enter the appropriate settings as defined in Table 7.

Step 8 Click **Save**.

Step 9 Use Cisco Unified Communications Manager Administration User Management to add an application user.

Step 10 Choose **User Management > Application User**.

Step 11 Click **Add New**.

Step 12 Enter the appropriate settings as defined in Table 8.

Step 13 Click **Save**.

Table 7 Fujitsu Mobile Access Manager SIP Device Configuration Settings

Field	Description
MAC Address	For example, 400000002050
Device Pool	Default
Phone Button Template	FJ-Standard MBL-AU
Device Security Profile	Fujitsu MBL-AU Standard SIP Non-Secure Profile
SIP Profile	Standard SIP Profile

Table 8 Fujitsu Mobile Access Manager SIP Application User Configuration Settings

Field	Description
User ID	For example, jtapiuser
Password	Enter a password of your choice.
Controlled Device	SEP400000002050
User Group	Standard CTI Enabled

Midcall Codec Support

Description

This feature allows Cisco Unified Communications Manager to handle changes in codec, IP address, or port information during an audio or video call. A new check box, **Require SDP Inactive exchange for mid-call media change,** in the SIP Profile Configuration window allows you to enable or disable sending mid-call media changes without breaking the existing media path with an inactive SDP.

Note This feature is applicable to mid-call reInvites coming from a peer SIP endpoint.

The mid-call codec feature supports:

- Change of codec in the mid-call Invite in audio/ video mlines.
- Change of IP address at the session level or mline level in audio/video mlines.
- Change of port in the mid-call Invite in audio/video mlines.

When you modify the codec, IP address, or port on the peer SIP endpoint during a call and enable the configuration by checking the **Require SDP Inactive exchange for mid-call media change** check box, Cisco Unified Communications Manager sends an inactive SIP invite to disconnect the current media channel at the peer SIP endpoint. Then it re-establishes the media path and sends an SDP containing the changes to the SIP line side device with incoming reInvite (or SIP trunk).

The inactive Invite gets sent because a Cisco Unified Communications Manager device may not support mid-call codec changes. When the device at the peer SIP endpoint detects a mid-call codec, IP address, or port change, it drops the call. Enabling the configuration check box has the effect of resetting the media path.

If the configuration is enabled, when the SIP trunk receives the SDP information with the modified codec, IP address, or port during a call, Cisco Unified Communications Manager disconnects the media path at the peer SIP endpoint and re-establishes the media path and sends the changed SDP information to the SIP trunk.

The default value of the check box specifies unchecked. If the check box remains unchecked, Cisco Unified Communications Manager does not disconnect the media. Instead, it passes the incoming changed SDP back to the peer SIP endpoint and lets it handle the changed information.

Note For those SIP devices that do not support SDP changes without breaking the media, the check box on the SIP Profile Configuration window can be checked. This way, Cisco Unified CM will first send an inactive SDP Invite to break the media path, followed by a reInvite with the changed SDP information.

Example

Phone A changes the port number mid-call by creating a new media description with the port number in the ‘m’ line. Though the change is sent, Phone A continues to listen for media on the old port until a response is received from the SIP trunk and media arrives on the new port. Ceasing to listen could result in loss of media during the transition.

If the updated stream is accepted by the SIP trunk, the SIP trunk begins sending traffic for that stream to the new port immediately. If the SIP trunk changes the port from the previous SDP, it must be prepared to receive media on both the old and new ports as soon as the answer is sent. The SIP trunk continues to listen for media on the old port until it arrives on the new port.

If the updated media stream is rejected, Phone A can cease being prepared to receive media on the new port soon after receiving the rejection. The procedure for changing the IP Address and port number are similar except that the connection line is updated for IP Address, not the port number.

Cisco Unified Communications Manager Administration Configuration Tips

The new **Require SDP Inactive exchange for mid-call media change** configuration check box in the SIP Profile Configuration window is applicable for SIP-to-SIP calls only.

You must enable the check box at the peer SIP endpoint. By default, this parameter specifies unchecked, which implies that the mid-call SDP can be forwarded as-is to the peer SIP. You are required to associate the newly created SIP Profile to the peer SIP Intercluster Trunk (SIP ICT).

GUI Changes

The **Require SDP Inactive exchange for mid-call media change** check box exists in the SIP Profile Configuration window.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

Migration from an older release to Cisco Unified Communications Manager 7.1(5) and later requires enabling or disabling the **Require SDP Inactive exchange for mid-call media change** check box in the SIP Profile Configuration window.

Using a SIP trunk, the new parameter in the SIP Profile Configuration window helps maintain backward compatibility with the releases prior to Cisco Unified Communications Manager 7.1(5) that are connected to Cisco Unified Communications Manager 7.1(5).

Note Cisco Unified Communications Manager supports mid-call codec update. But if a codec change exists in the new offer, you will be required to set up the media again.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

The Import/ Export tool supports enable and disable of the **Require SDP Inactive exchange for mid-call media change** check box on the SIP Profile Configuration window.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

The following are important points to remember when you use this feature:

- The feature is applicable only to mid-call reInvites coming from a peer SIP endpoint.
- If there is a codec or IP address change in the SIP trunk in the non-inactive mid-call invite, Cisco Unified Communications Manager disconnects media at the peer SIP endpoint. While the new SDP is negotiated, the SIP trunk might experience a temporary pause. During this pause, no packets will flow in or out of the old port of the peer SIP. When the two-way media channels are negotiated at the peer SIP side and the SIP trunk receives an answer, the two-way RTP begin flowing between the new ports.
- If there is a port change in the SIP trunk in the non-inactive mid-call invite, and if the peer SIP side is MGCP or SCCP device, the SIP trunk continues to send packets to the old port but may not receive packets from the old port for a small duration during the re-opening of channels. When the channels are re-opened on the peer SIP side and the SIP trunk receives an answer, it begins receiving RTP packets on the new port.
- If the peer SIP endpoint is a SIP or H.323 device, the SIP trunk might experience a temporary pause during which two way channels are reopened on the peer SIP side.

Unrestricted Export Support

The restricted US export classification on Cisco Unified CM meant that governmental and military customers in many countries could not employ Unified CM in their networks.

In addition to the delay inherent in obtaining export licenses, products classified as restricted by the Department of Commerce (DoC) carry a requirement to allow US government representatives to demand on-site inspections at any time to confirm that the product is being used in accordance with its licensed purpose. This post-shipment verification (PSV) is unacceptable to many customers.

Additionally, some foreign countries maintain import restrictions which prohibited Unified CM from being available to customers in those countries. Both US export and foreign import issues stem from Unified CM support for strong encryption of signaling and media.

Unrestricted Classification

Because Cisco has obtained an unrestricted classification from the DoC for a version of Unified CM, beginning with Unified CM 7.1(5), both restricted and unrestricted versions of Unified CM will be released in parallel.

Limitations

Signaling and media encryption is permanently disabled in the unrestricted version, but remains unchanged in the restricted version.

Migration from the unrestricted version to the restricted version is not supported.

Note No impact exists to other security features such as HTTP(s), SSH, password encryption and authentication (for example, SIP digest authentication), mechanisms used by unrestricted Unified CM clients such as JTAPI, TSP, encryption of SNMP traffic, encryption of data related to database that is done by using IPSEC and IMS on the server side.

The communication between CTL client and provider remains encrypted.

Universal IOS Transcoding

Description

Cisco Unified Communications Manager 7.1(5) and later leverages the IOS-based DSP universal transcoding to do codec conversion between a wide range of codec combinations to enable disparate endpoints to communicate with each other.

In earlier releases, Cisco Unified Communications Manager used only a subset of the IOS-based DSP transcoding capability, requiring that one side of the connection had to be G.711. Cisco Unified Communications Manager now allows all types of transcoding requests to IOS-based DSP transcoders. It detects transcoders capable of doing universal transcoding and allocates these resources for any-to-any transcoding requests.

Note The universal transcoder does not support all the standard codecs that are currently available. It can transcode between supported codec types only.

Example

Phone A (which supports only G723) calls Phone B (which supports only G729). After the initial call handling, when Cisco Unified CM tries to establish media between the two phones, it discovers the need for a transcoder to convert G723 to G729.

Cisco Unified Communications Manager finds a Dixieland-based Universal Xcoder in the available resources pool and allocates it for this call. The Universal Xcoder is capable of converting the media to and from G723 and G729 and, thus, starts streaming to the phones after receiving OLC (Open logical channel) and SMT (Start media transmission) signals from Cisco Unified Communications Manager.

Cisco Unified Communications Manager Administration Configuration Tips

You configure and register a Dixieland Universal Transcoder the same way as the regular Dixieland Transcoder. During the registration with Cisco Unified Communications Manager; however, the Universal Transcoder includes an extra capability (Media payload type 222) to indicate that it supports Universal Transcoding.

Example

On the IOS server, ‘DSPFarm Profile 100 Transcode’ will be suffixed with ‘Universal’ after configuration. So, the profile name will read: ‘DSPFarm Profile 100 Transcode Universal.’

GUI Changes

No GUI changes for this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade considerations for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

None.

Cisco Mobile 8.0 Support

Cisco Unified Communications Manager supports SIP base dual-mode mobile phones with Cisco Mobile 8.0. Cisco Unified Communications Manager supports the new *Cisco Dual Mode for iPhone* device type for iPhone, which specifies a SIP-based dual-mode mobile phone that is capable of leveraging VoIP connectivity over the enterprise WLAN.

Cisco Unified Communications Manager supports dual-mode mobile phones that use the Cisco Unified Mobile Communicator client and SIP protocol within the WLAN. Cisco Unified Communications Manager must handle dual SIP registrations (one from Cisco Unified Mobile Communicator via Cisco Unified Mobility Advantage and one from Wi-Fi as a SIP endpoint).

Cisco Mobile 8.0 provides iPhone users with voice over IP (VoIP) calling, visual voicemail, and access to the corporate directory while users are connected to the corporate network over Wi-Fi, either on premises or over VPN. Cisco Mobile 8.0 specifies an IP telephony endpoint that associates with Cisco Unified Communications Manager.

Note Cisco Mobile 8.0 is distinct from the Cisco Mobile application that runs in conjunction with a Cisco Unified Mobility Advantage server.

In order for Cisco Unified Communications Manager to support Cisco Mobile 8.0, Cisco Unified Communications Manager administrators must take at least the following step:

1. Configure the new device in Cisco Unified Communications Manager Administration.

The *Administration Guide for Cisco Mobile 8.0 for iPhone* provides the details of the complete configuration that is required to configure Cisco Mobile 8.0, including the steps that must be performed in Cisco Unified Communications Manager Administration. Refer to the document at the following URL:

http://www.cisco.com/en/US/products/ps7271/prod_installation_guides_list.html

In-Service Upgrade Enhancements for Cisco Unified IP Phones 8961, 9951, and 9971

Description

The Cisco Unified IP Phone 8961, 9951, and 9971 uses the dual-banked firmware memory to compensate for increased firmware load size. Dual-banked firmware memory allows the phone to download the firmware upgrade while remaining in service.

Prior to Release 7.1(5), the Cisco Unified CM administrator had to specify the firmware load for the phone by using the Device Defaults Configuration window or by using the phone settings. The IP phone would then download the firmware to the Inactive firmware bank in the background; the phone continued to provide service by using its Active firmware load.

Cisco Unified CM administrators can specify the firmware load for both the Active and Inactive firmware banks for the Cisco Unified Communications Manager Release 7.1(5) and later. A new **Switch Loads** function will swap the Active and Inactive settings and continue to control both the settings while preserving the former Active setting in the Inactive entry.

Enabling the independent image download and switchover enhances control of dual-banked firmware supporting device types and allows the Cisco Unified CM administrator greater control and visibility during the download of the dual-banked phone firmware and switchover. Administrators can:

- Control the download of the dual-banked phone firmware and switchover, while retaining backward compatibility.
- Alter the Inactive image setting to initiate an image download only.
- Implement separate switch load requests to cause the phone to start using a previously downloaded Inactive firmware load while preserving the Active load designation as the new Inactive image.
- Use independent Switch Loads to implement a revert function when a newly installed firmware load does not behave as desired.

The Cisco Unified CM administrator can upload the new firmware before the upgrade. The new firmware (a COP file) is uploaded by using Cisco Unified Communications Operating System, Software Uploads.

Note The dual-banked firmware update feature allows Cisco Unified CM administrator to upgrade phone firmware with a new load before resetting the new load to an Inactive load status. Instead of waiting for all the phones to download the firmware, Cisco Unified CM administrators can use the **Switch Loads** function to quickly switch from the old load to the new load in less time.

Upgrading the dual-banked firmware reduces the bandwidth congestion and the delay in download during system maintenance while allowing Cisco Unified CM administrators to determine when to set the new firmware to Active load.

Cisco Unified Communications Manager Administration Configuration Tips

The Unified CM administrator can verify whether the Active and Inactive loads were swapped correctly.

To swap the firmware load that is running on the IP phone (for example, from Load A to Load B), follow these steps:

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device > Device Defaults**. Save the Inactive version for a phone that supports Dual-Bank feature.

Step 2 In Cisco Unified OS Administration, choose **Software Upgrades > Install/Upgrade** and upload the COP file for Load B.

Step 3 In Cisco Unified CM Administration, go to **Device > Device Defaults**.

The Dual-Bank Information area indicates Load A as the Inactive load and Load B as the Active load.

Step 4 Click **Swap Loads** to swap Load A and Load B.

The Dual-Bank Information area indicates Load A as the Active load and Load B as the Inactive load.

Step 5 Click **Save** to save the configuration settings. All the phones will run with Load B as Inactive load.

Step 6 In Cisco Unified CM Administration, go to **Device > Phone**.

Step 7 Change Load B to Active load. This changes the Load A to an Inactive load.

Step 8 Click **Save**.

The Load B is Active and the Load A is Inactive.

Note During dual-banked firmware upgrade, the previous Active load will be swapped as an Inactive load. No change will be made if the new load matches with the Active load settings. If there is no previous Active load, (fresh install), the Inactive load setting will be left empty.

GUI Changes

A new area in the **Device Defaults Configuration** (Device > Device Settings) window allows you to monitor and change the **Dual Bank Information** (for dual-banked firmware capable devices only).

Table 9 describes the fields in the **Dual Bank Information** area.

Table 9 Dual Bank Information area fields

Field	Description
Device Type	Specifies the type of device for which device defaults can be set.
Protocol Session Initiation Protocol (SIP)	Specifies the protocol that the corresponding device in the Device Type column uses.
Load Information	Specifies the ID number of the firmware load that is used with a particular type of hardware device. If you install an upgrade or patch load, you must update the load information for each type of device that uses the new load.
Inactive Load Information	Specifies the ID number of the Inactive firmware load.
Device Pool	Specifies the device pool that is associated with each type of device. The device pool defines common characteristics for all devices in the pool.
Phone Template	Specifies the phone button template that each type of Cisco Unified IP Phone uses. The template defines what keys on the phone perform that function.

In the **Dual Bank Information** area in the **Device Defaults Configuration** (Device > Device Settings) window, there is a new Swap Loads icon. Administrators can override the default installation of new firmware as the Active load by using the Switch Loads operation prior to execution of the **Apply Config**. This will move the new firmware load to the Inactive load setting restoring the previous Active load setting.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install or upgrade to Cisco Unified Communications Manager 7.1(5), you can use this feature.

COP file or system install/upgrade operations will remain unaltered with the following exceptions related to devices supporting Dual-Banked firmware and **Apply Config** features:

2. The existing Active firmware load designation in the Device Defaults will be preserved by copying it to the Inactive firmware load setting prior to marking of the new firmware as the Active load.

Note If the new load already matches the active load setting, then no change will be made to either the Active or the Inactive loads.

3. The Cisco Unified CM administrator may set the newly downloaded firmware as the Inactive load, restoring the Active load setting from the Inactive bank setting. This would cause the phone to download the new firmware to its Inactive bank. The administrator can later switch the phones to use the new load as the Active load with no download delay.

Note This would be accomplished via the **Device Defaults** web page. There the administrator can use the **Switch Loads** icon to swap the Active and Inactive loads prior to an **Apply Config** request or device reset/restart. This will restore the current load as the configured Active Load and place the newly installed firmware into the configured Inactive Load.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

BAT is able to accept load information as previously for the Active load, load information for the inactive load, or both. BAT import/export tool supports this feature.

To verify the BAT export of device defaults, follow these steps:

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device > Device Defaults**.

Check the load information in the **Inactive Load Information** field.

Step 2 From the **Bulk Administration > Import/Export > Export > Device Defaults** window, schedule an export job.

Step 3 Download the exported tar file.

Step 4 Untar the file and check the file format in the exported csv file.

Step 5 Check whether the .csv file has a column for “Inactive Load Information” with correct value.

The .csv file value must match with the Device Default value in the Cisco Unified CM Administrator window.

To verify the BAT import of device defaults with overrides, follow these steps:

Note You can only update the Device Default settings.

Procedure

Step 1 Upload the exported tar file to Cisco Unified CM.

Step 2 From the **Bulk Administration > Import/Export > Import** window, select the file to upload from the drop-down list.

Step 3 Check the override check box and schedule an Import Job.

Step 4 In Cisco Unified CM Administration, choose **Bulk Administration > Job Scheduler** window, check the job status.

Step 5 From the **Device > Device Defaults** window, verify whether the given field is updated properly.

The Device Defaults fields will be updated as specified in the csv file.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

None.

Security

This section contains information about the Security Icon Enabled by Phone Model feature.

Security Icon Enabled by Phone Model

Beginning with Cisco Unified Communications Manager Release 7.1(3), Cisco Unified Communications Manager allows Security icons to be enabled by phone model on Cisco Unified IP Phones. The Security icon indicates whether the call is secure and the connected device is trusted.

A Trusted Device represents a Cisco device or a third-party device that has passed Cisco security criteria for trusted connections. This includes, but is not limited to, signaling/media encryption, platform hardening, and assurance. If a device is trusted, a Security icon displays, and a secure tone plays on supported devices. Also, the device may provide other features or indicators that are related to secure calls.

Cisco Unified Communications Manager determines whether a device is trusted when you add it to your system. The security icon displays for information purposes only, and the administrator cannot configure it directly.

Beginning with Cisco Unified Communications Manager Release 7.1(3x), Cisco Unified Communications Manager also indicates whether a gateway is trusted by displaying an icon and a message in Cisco Unified Communications Manager Administration.

This section describes the behavior of the security icon for trusted devices on both the Cisco Unified IP Phones and in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration

The following windows in Cisco Unified Communications Manager Administration indicate whether a device is trusted:

CTI Route Point Configuration

The CTI Route Point Configuration window (**Device > CTI Route Point**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Voice Mail Port Configuration

The Voice Mail Port Configuration window (**Advanced Features > Voice Mail > Cisco Voice Mail Port**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Gateway Configuration

For each gateway type, the Gateway Configuration window (**Device > Gateway**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Phone Configuration

For each phone device type, the Phone Configuration window (**Device > Phone**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted. For a list of trusted Cisco Unified IP Phones, see the "Trusted Devices" section on page 50.

Cisco Unified IP Phones

Beginning with Cisco Unified Communications Manager Release 7.1(3x), the type of device that a user calls will affect the security icon that displays on the phone. Previously, the system set the security icon by determining whether the signalling and media were secure. For Release 7.1(3x), the system will consider the following three criteria to determine whether the call is secure:

- Are all devices that are on the call trusted?
- Is the signaling secure (authenticated and encrypted)?
- Is the media secure?

Before a supported Cisco Unified IP Phone displays the Lock Security icon, be aware that all three criteria must be met. For calls that involve a device that is not trusted, regardless of signaling and media security, the overall status of the call will stay unsecure, and the phone will not display the Lock icon. For example, if you include an untrusted device in a conference, the system considers its call leg, as well as the conference itself, to be unsecure.

Trusted Devices

For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports this Cisco Unified Communications Manager release or the firmware documentation that supports your firmware load.

You can also use Cisco Unified Reporting to list the phones that support a particular feature. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

Bulk Administration Tool

This section provides the following information:

- In Unrestricted Unified CM, Do Not Edit These Default Field Values, page 50

In Unrestricted Unified CM, Do Not Edit These Default Field Values

If your Cisco Unified Communications Manager is unrestricted, Cisco recommends that you do not edit the following default field values of the Import/ Export configuration feature in BAT:

- Configuring a Phone Security Profile
- Cisco IOS Conference Bridge Configuration Settings
- Configuring Voice Mail Port Wizard
- Configuring Voice Mail Port

Cisco Unified IP Phones

This section provides the following information:

- Assisted Directed Call Park on TNP devices, page 51

Assisted Directed Call Park on TNP devices

Description

Assisted directed call park is supported on the following Cisco IP Phone models:

- Cisco Unified IP Phone7931
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7975
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

. Assisted directed call park means that the end user only needs to press one button to direct-park a call. This requires you to configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call will be immediately parked at the Dpark slot associated with the Directed Call Park feature button.

Cisco Unified Communications Manager Administration Configuration Tips

For assisted directed call park to work, you must configure a BLF Directed Call Park button.

GUI Changes

There are no GUI changes for this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.0(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Cisco Unified Serviceability

This section contains information on the following topics:

Audit Log Records User Logout Events

In earlier releases of Cisco Unified Communications Manager, when you logged in to Cisco Unified Communications Manager Administration, performed required tasks and logged out, the log in event got recorded in the audit logs but the logout event did not get recorded.

Cisco Unified Communications Manager 7.1(5). resolves this issue.

To see the log in and log out events, check the audit logs from **RTMT > Trace & Log Central > Real Time Trace >Audit Logs**.

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 7.1 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 7.1(5) As of April 10, 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 7.1(5) As of April 10, 2010" section on page 54 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.

- 7.0(2.20000-x) = Cisco Unified Communications Manager Release 7.0(2a)
- 7.0(2.10000-x) = Cisco Unified Communications Manager Release 7.0(2)
- 6.1(3.3000-1) = Cisco Unified Communications Manager 6.1(3b)
- 6.1(3.2000-1) = Cisco Unified Communications Manager 6.1(3a)
- 6.1(3.1000-x) = Cisco Unified Communications Manager 6.1(3)
- 5.1(3.7000-x) = Cisco Unified Communications Manager 5.1(3f)

Note Because defect status continually changes, be aware that the "Open Caveats for Cisco Unified Communications Manager Release 7.1(5) As of April 10, 2010" section on page 54 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 53.

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 7.1(5) As of April 10, 2010

The following information comprises unexpected behavior (as of April 10, 2010) that you may encounter in Release 7.1(5) of Cisco Unified Communications Manager.

Table 10 Open Caveats for Cisco Unified Communications Manager Release 7.1(5) as of April 10, 2010

Id	Component	Headline
CSCtg12030	cli	'utils fior enable' starts the fior module/service immediately
CSCtg04028	cli	'utils fior [start/stop]' date parameter not accepted.
CSCsr30432	cmcti	c2conf: Cisco Unified CM does not send NOTIFY.
CSCtd03506	cmcti	Implementing ScbId for DirectTransferReq and LineCallJoinReq.
CSCtg04215	cmui	UI issue exists in Device Mobility when Home and Roaming DMG set to None
CSCte41148	cmui	ETSGJ-CH: IE window minimizes automatically when you click the Modify button.
CSCtg09132	cp-h323	Incorrect PID format for SdlTcpConnection, Null PID in TcpStopSessionInd.
CSCtf57240	cp-mediacontrol	IPv6: CUVA(ds) receives a reorder when calling over v6-SIP ICT.

Table 10 Open Caveats for Cisco Unified Communications Manager Release 7.1(5) as of April 10, 2010

CSCtf94005	cp-mediacontrol	Cisco Unified CM terminates CTMS call if mode is inactive until payload matched.
CSCtf71611	cp-mediacontrol	0 IP Address populated when MTP gets invoked between MOH and H323.
CSCtf98540	cp-mobility	Gateway Calling Party Transformation fails on RDP with Ext phone number mask.
CSCtg07896	cp-mobility	Need exists to populate SIP Reason for the Mobility IVR.
CSCtf99027	cp-resourcecontrol	MTP resource leak : deallocate with cleartype while channel already closed.
CSCtg04283	cp-sip-trunk	SIP trunk session refresh changes SDP direction.
CSCtg01244	cp-ss-mwi	MWI using enhanced MWI method (StationMwiNotification) across QSIG fails.
CSCtb92983	cpi-os	Publisher server gets stuck when it boots (kenerl panic) after switch-version from.
CSCtd99795	cpi-os	If NIC teaming is enabled, the netdump server does not work.
CSCta74144	cpi-os	Multiple FAILEDs in U1 upgrade because shutdown process not running.
CSCsz55537	ext-mobility	JPN:Katakana strings on Extension Mobility screens.
CSCtd14027	security	IMPORTANT TLS/SSL SECURITY UPDATE - JDK
CSCte67321	smdiservice	CMI requires server reboot to start.
CSCsu26261	tapisdk	TSP auto upgrade fails on Vista client.
CSCte21931	voice-sipstack	Cisco Unified CM incorrectly sends INVITE when handling CcNotifyReq.
CSCtf09981	voice-sipstack	Cisco Unified CM does not try to re-establish the TCP connection when receiving RST.

Documentation Updates

This section contains information on documentation omissions, errors, and updates for the following Release 7.1(3) documentation, which is our latest documentation set:

Installation, Upgrade, and Migration

This section contains information on the following topics:

Installing Licenses While Replacing a Publisher Node

This section replaces the section "Replacing the Publisher Node" in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*. Follow this process to replace a publisher server with a new server.

Table 11 Replacing the Publisher Node Process Overview

	Description	For More Information
Step 1	Perform the tasks in the "Server or Cluster Replacement Preparation Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*
Step 2	Gather the necessary information about the old publisher server.	See the "Gathering System Configuration Information to Replace or Reinstall a Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 3	Back up the publisher server to a remote SFTP server by using the Disaster Recovery System and verify that you have a good backup.	See the "Creating a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 4	Get new licenses of all the license types before system replacement.	Get new licenses of all the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. You only need new licenses if you are replacing the publisher node. For more information, see the "Obtaining a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 5	Shut down and turn off the old server.	
Step 6	Connect the new server.	
Step 7	Install the same Cisco Unified Communications Manager release on the new server that was installed on the old server, including any Engineering Special releases. Configure the server as the publisher server for the cluster.	See the "Installing Cisco Unified Communications Manager on the New Publisher Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 8	Restore backed-up data to the publisher server by using Disaster Recovery System.	For more information, see the "Restoring a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 9	Reboot all nodes in the cluster. If the server is not in a cluster, then reboot the server.	

	Description	For More Information
Step 10	Upload all of the new license files to the publisher server.	Upload new license files for all of the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. For more information, see the "Uploading a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 11	Delete all invalid license files (those based on the old server MAC address).	"Deleting Invalid License Files" section on page 57
Step 12	Perform the post-replacement tasks in the "Post-Replacement Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*

Deleting Invalid License Files

The license files that get restored to the server by Disaster Recovery System are invalid because they are bound to the MAC address of the old server. To delete all invalid license files from your server, follow these steps:

Step 1 Obtain the MAC address of the new server by running the **show status** CLI command.

The MAC address displays in the field License MAC.

Step 2 View each license file on the server to determine which license files are invalid.

a. In Cisco Unified Communications Manager Administration, choose **System > Licensing > License File Upload**.

b. Choose a license file from the Existing License Files drop-down list.

c. Click the **View File** button.

d. The license file MAC address displays in the HOSTID field.

If the license file MAC address does not match the server MAC address, then the license is invalid.

e. Record the file name of each invalid license file.

f. Repeat this process for each license file on the server.

Step 3 Delete each invalid license file from the server by running the CLI command **file delete license** *filename*, where *filename* is the name of the license file.

For more information about this command, refer to the document *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Server Replacement

This section contains information on the following topics:

Password Validation During a Server Replacement

If you replace a server that was previously upgraded from an older product release, the Cisco Unified Communications Manager installation program may deny your passwords. This happens because the password validation rules might get stronger in the new product release, but passwords do not get revalidated during an upgrade; however, when you perform a fresh installation on the server that you are replacing, the new, stronger password validation occurs.

If this happens, choose new passwords that the installation program will accept. For more information about passwords, see the document *Installing Cisco Unified Communications Manager*.

Rebooting Servers While You Are Replacing a Publisher Server

This section comprises an update to the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager Release 7.1(2)*. It applies to the procedure for replacing a publisher server in a cluster.

After you restore data to the new publisher server, reboot all the cluster nodes. The document says to reboot just the publisher server, but you must reboot all of the cluster nodes to enable database replication.

Troubleshooting

This section contains information on documentation omissions, errors, and updates for the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Two New dbreplication Commands Exist

The *Troubleshooting Guide for Cisco Unified Communications Manager* omits two dbreplication commands.

utils dbreplication runtimestate

Use this command

- To determine the status of a replication reset.
- Along with **utils dbreplication status** | **utils dbreplication quickaudit**, to determine the general health of replication.

utils dbreplication quickaudit

Use this command to run a quick database check on selected content on dynamic tables.

Bulk Administration Tool

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Bulk Administration Guide*.

The following information is missing from the online help for *Cisco Unified Communications Manager Bulk Administration Guide*:

Deleting Unassigned Directory Numbers

Use the following procedure to delete unassigned directory numbers by creating a query to locate the phone records.

Procedure

Step 1 Choose **Bulk Administration > Phones > Delete Phones > Delete Unassigned DN**.

The Delete Unassigned Directory Numbers window displays.

Step 2 From the first Delete Bulk Unassigned Directory Number where drop-down list box, choose one of the following criteria:

- Pattern
- Description
- Route Partition

From the second Delete Bulk Unassigned Directory Number where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable.

Step 4 Click **Find**.

A list of discovered phones displays by

- Pattern
- Description
- Partition

Tip To find all unassigned directory numbers that are registered in the database, click **Find** without entering any search text.

Step 5 In the Job Information area, enter the Job description.

The default description is Delete Unassigned DN - Query

Step 6 To delete the unassigned directory numbers immediately, click the Run Immediately radio button. To delete the phone records at a later time, click Run Later.

Step 7 To create a job for deleting the phone records, click **Submit**.

Note Make sure to browse the entire list of displayed results before submitting the job.

Step 8 To schedule and/or activate this job, use the Job Configuration window.

Cisco Unified Communication Manager CDR Analysis and Reporting

This section contains information on documentation omissions, errors, and updates for the *CDR Analysis and Reporting Administration Guide*.

Changed Values of Mobility Cell Pick

The Mobility section of "CDR Examples" chapter in the *Cisco Unified Communications Manager Call Detail Records Administration Guide*has wrong values for some field names. The corrected values follow:

Field Names	Enterprise Call to 22285	Server Call to Cell Phone	Final Handout Call
callingPartyNumber	22202	2202	22202
originalCalledPartyNumber	22285	22285	22285
finalCalledPartyNumber	22285	9728324124	22285
lastRedirectDn	22285	22285	22285
origCause_Value	393216	393216	0
dest_CauseValue	393216	393216	16
lastRedirectRedirectReason	0	0	415
lastRedirectRedirectOnBehalfOf	0	24	24
joinOnBehalfOf	0	24	24

Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting

The *CDR Analysis and Reporting Administration Guide* omits the following statement about the primary purpose of the Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) software:

> CAR is not intended to replace call accounting and billing solutions that third-party companies provide. You can find the companies that provide these solutions and that are members of the Cisco Technology Developer Program by searching the home page of the Cisco Developer Community at this URL: http://developer.cisco.com/web/cdc/home.

The following online document has been revised to include the omitted statement:

- book: *CDR Analysis and Reporting Administration Guide, Release 7.1(2)*
  chapter: CDR Analysis and Reporting Overview

"Mailing a Report" Recipients

The "Mailing a Report" chapter in the *Cisco Unified Communications Manager Call Detail Records Administration Guide* omits this information:

When the Mailing option gets enabled,

- End users receive the individual billing summary.

- Managers receive the individual billing summary, department billing summary, Top n Report, and the QoS report.
- CAR Administrators receive all reports.

Cisco Unified Communications Manager Security

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Security Guide*.

You Can Use HTTPS Protocol with Different Browsers and Operating Systems

The *Cisco Unified Communications Manager Security Guide* incorrectly states that the HTTPS is only compatible with Microsoft Windows products. The following paragraph provides the corrected information:

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a compatible browser and web server. HTTPS uses certificates to ensure server identities and to secure the browser connection.

Definition of Locally Significant Certificate

The definition of Locally Significant Certificate (LSC) in the *Cisco Unified Communications Manager Security Guide* need correction as follows: A third-party certificate authority (CA) cannot issue an LSC. An LSC represents a digital X.509v3 certificate that CAPF issues. It gets installed on a phone or JTAPI/TAPI/CTI application.

Cisco Unified Communications Operating System

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Operating System Administration Guide*.

Incorrect Values for Phase One DH and Phase Two DH

The Security chapter of the *Cisco Unified Communications Operating System Administration Guide* incorrectly specifies the values for Phase One DH and Phase Two DH. On the IPSEC Policy Configuration window, the Phase One DH and Phase Two DH pulldown menus contain the values 2, 1, and 5.

Using Certificates Issued by a Third-Party Certificate Authority

This information supplements the documentation about using certificates that are issued by a third-party certificate authority (CA) that is in the *Cisco Unified Communications Operating System Administration Guide*.

- For all certificate types except CAPF, obtain and upload a CA root certificate and an application certificate on each node.
- For CAPF, obtain and upload a CA root certificate and an application certificate only on the first node.
- CAPF and Cisco Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:
  - The CAPF CSR uses the following extensions:

    ```
    X509v3 extensions:
    X509v3 Key Usage:
    Digital Signature, Certificate Sign
    X509v3 Extended Key Usage:
    TLS Web Server Authentication, IPSec End System
    ```

  - The CSRs for Cisco Unified Communications Manager, Tomcat, and IPSec use the following extensions:

    ```
    X509v3 Key Usage:
    Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
    X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
    ```

- Upload the CA root certificate of the CA that signed an application certificate. If a subordinate CA signs an application certificate, you must upload the CA root certificate of the subordinate CA, not the root CA.
- You upload CA root certificates and application certificates by using the same Upload Certificate dialog box. When you upload a CA root certificate, choose the certificate name with the format *certificate type*-**trust**. When you upload an application certificate, choose the certificate name that only includes the certificate type. For example, choose **tomcat-trust** when you upload a Tomcat CA root certificate; choose **tomcat** when you upload a Tomcat application certificate.
- When you upload a CAPF CA root certificate, it gets copied to the CallManager-trust store, so you do not need to upload the CA root certificate for CallManager separately.

Revised Procedure to Shut Down the System

The "System Restart" chapter in the *Cisco Unified Communications Operating System Administration Guide* requires the following revisions to the Shut Down the System section:

- Replace the text of the first caution with the following text:

  Do not press the power button on the server to shut down the server or to reboot the server. If you do, you may accidentally corrupt the file system, which may prevent you from being able to reboot your server.

- Replace the text after the first caution with the following text:

  To shut down the system, follow Procedure 1 or Procedure 2.

- Replace the note text with the following text:

The hardware may require several minutes to power down.

- Insert the following text after the note:

  Procedure 2

  Run the CLI command **utils system shutdown** or the command **utils system restart**. For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Cisco Unified Communications Manager Administration

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager Features and Services Guide*, and the *Cisco Unified Communications Manager System Guide*.

Cisco Unified Communications Manager Administration Guide

Cisco Unified Communications Manager System Guide

Cisco Unified Communications Manager Features and Services Guide

- IPv6 Chapter Does Not Contain Information on NTP Server, page 79
- Mobile Voice Access Directory Number Field Description, page 80
- Changed Values of Mobility Cell Pick, page 60

Enabling AAR for Hunt Pilots

The AAR Group field in the Hunt Pilot Configuration table in the "Hunt Pilot Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly includes this note:

> You can enable AAR for this hunt pilot only if all members of the line group are in the same location.

That is incorrect. You can configure hunt pilots pointing to hunt lists that have line group members in different locations.

Description of the Reset Button

The Cisco Unified Communications Manager Configuration Settings section of the “System Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide* contains incomplete description of the Reset button. The description should comprise:

Click this button to reset all devices that belong to the same Cisco Unified CM Group as this Cisco Unified Communications Manager server.

Note All devices in the Cisco Unified CM Group of which this server is a member get reset, not just those devices that are registered with this server.

Circular Algorithm Description Is Incorrect

The Line Group Configuration Settings table in the “Line Group Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide* contains this description of the Circular Algorithm:

> Circular-If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which Cisco Unified Communications Manager most recently extended a call. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group.

The description should say:

> Circular-If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the next sequential member in the list who is either idle or busy but not "down”. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group.

Administrator Can Set User Credential Policy to Expire Without Making a Global Policy Change

The Credential Settings and Fields section of the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly includes the following information:

For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

And, again, regarding the Does Not Expire checkbox:

You cannot uncheck this check box if the policy setting specifies Never Expires.

For releases above 6.1(3), this is not true. An administrator can set a user credential policy to expire without making a global policy change.

How the Number of Client Matter Codes Affects System Start Up Time

The "Client Matter Codes" chapter of the *Cisco Unified Communications Manager Administration Guide* omits the following information:

Because the number of CMCs directly impacts the time that is required for Cisco Unified Communications Manager to start up, limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires approximately 1 hour to start up; a system with 1 million CMCs requires approximately 4 hours to start up.

SIP Profile Configuration No Longer Includes a Call Stats Check Box

The SIP Profile Configuration Settings section of the "SIP Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* includes information about the Check Stats check box.

That check box no longer exists.

NTP Reference Configuration Settings Omits Two Available Modes

The Phone NTP Reference Configuration Settings section of the "System Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* omits information about two available Modes.

The additional information specifies:

- Multicast
- Anycast

IP Subnet Example Incorrectly Contains a Period (.) Instead of a Slash (/)

The "SIP Route Patterns Configuration Settings" chapter of the *Cisco Unified Communications Manager Administration Guide* contains the following examples:

IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18.21 (IP subnet).

The examples should specify:

IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18/21 (IP subnet).

Default Setting of the User Must Change at Next Login Check Box Is Incorrect

The "User Management Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* contains incorrect information about the default setting of the User Must Change at Next Login check box.

The correct information is that the default setting for this check box specifies checked.

Device Name Field Omits Information About Valid Characters and Number of Characters Allowed

The Phone Configuration Settings section of the "Cisco Unified IP Phone Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include information about valid characters for the Device Name field. That information follows:

Enter a name to identify software-based telephones, H.323 clients, and CTI ports.

For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases you can use dot (.), dash (-), and underscore (_) as well.

Note Because the rules for the device name field depend on the device type, Cisco recommends that you refer to the product documentation to determine which character set is valid for your device, as well as the number of characters allowed.

Valid Characters Not Included in the Description of the Transcoder Device Name Field

The Transcoder Configuration Settings section of the "Transcoder Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* did not include the characters that are allowed in the Device Name field.

That information follows:

You can enter up to 15 characters in the Device Name field. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-) and underscore (_).

Valid Characters Not Included in the Description of the IOS Conference Bridge Name Field

The IOS Conference Bridge Configuration Settings section of the "Conference Bridge Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include the characters that are allowed in the Device Name field.

That information follows:

You can enter up to 15 characters in the Device Name field. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-) and underscore (_).

Invalid Characters for Cisco Conference Bridge (WS-SVC-CMM) Description Field Omitted

The Description field in the Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings section of the "Conference Bridge Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include the invalid characters.

Invalid characters comprise quotes (“), angle brackets (<>), backslash (), ampersand,(&), and percent sign (%).

Application Dial Rule Configuration Settings Table Is Incorrect

The Application Dial Rule Configuration Settings table in the "Application Dial Rules Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* contains some incomplete and erroneous information. The correct information follows.

Table 12 Application Dial Rule Configuration Settings

Field	Description
Name	Enter a name in the Name field. The name must be at least one character in length and can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Ensure each application dial rule name is unique.
Description	Enter a description of the application dial rule in the Description field. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>)
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid characters include numeric digits (0-9), plus sign (+), asterisk (*), and number sign (#). Be aware that you cannot enter more than 50 characters in this field.
Number of Digits	Enter the length of the dialed numbers to which you want to apply this application dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100.
Total Digits to be Removed	Enter the number of digits that you want Cisco Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100. • Cannot contain a value that is more than the value in the Number of Digits field.
Prefix With Pattern	Enter the pattern to prepend to dialed numbers that apply to this application dial rule. Valid values include numeric digits (0-9), plus (+), asterisk (*), and pound (#). Be aware that you cannot enter more than 50 characters in this field.
Application Dial Rule Priority	Choose the dial rule priority as top, bottom, or middle.

Valid Characters for Voice Mail Profile Name Field Omitted

In the Voice-Mail Profile Configuration Settings section of the "Voice Mail Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*, the description of the Voice Mail Profile Name field does not include information about valid characters.

The valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), period(.), dash(-), underscore(_).

Meet-Me Number/Pattern Configuration Settings Description Field Description Is Incorrect

The Meet-Me Number/Pattern Configuration Settings section in the "Call Routing Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can enter up to 30 alphanumeric characters in the description field. In fact, you can enter up to 50 alphanumeric characters.

User Documentation Misnames Single Button Barge Field

The Device Profile Configuration Settings section in the "Device Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly calls the Single Button Barge field, Single Button Barge/cBarge.

The description of that field also incorrectly includes information about cBarge.

Allowed Prefix Digits Incorrect for AAR Group Configuration

The AAR Group Configuration Settings section in the "Call Routing Configuration" chapter of the Cisco *Cisco Unified Communications Manager Administration Guide* incorrectly enumerates the valid characters that are allowed in the Prefix Digits field.

The characters that are allowed comprise numeric characters (0-9), alpha characters (A - D), asterisk (*), pound sign (#), plus sign (+), and dash (-).

Service Parameters Expanded Explanation

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

To configure service parameters, you must select a single server and a single service on that server. After you make the selection you can configure parameters for the service on that single serve and on others that apply to the service on all servers within the cluster; these get marked as clusterwide.

Unlike enterprise parameters that apply to all services, each service gets configured with a separate set of service parameters.

Do Not Begin Starting and Ending Directory Numbers with a Zero (0)

In the *Cisco Unified Communications Manager Administration Guide*, in Table 3 of the "Cisco Unified Communications Manager Configuration" chapter, under Auto-registration Information, the descriptions of Starting Directory Number and Ending Directory Number omit the information that neither number should begin with a zero (0).

Number of Locations and Regions That Cisco Unified Communications Manager Supports

The Cisco Unified Communications Manager Administration documentation incorrectly states the number of locations and regions that Cisco Unified Communications Manager supports. The correct limits follow:

- Cisco Unified Communications Manager supports up to 2000 locations.
- Cisco Unified Communications Manager supports up to 2000 regions.

The following online documents have been revised with the correct limits:

- book: *Cisco Unified Communications Manager Administration Guide, Release 7.1(2)*
  chapter: Location Configuration
- book: *Cisco Unified Communications Manager Administration Guide, Release 7.1(2)*
  chapter: Region Configuration
- book: *Cisco Unified Communications Manager System Guide, Release 7.1(2)*
  chapter: System-Level Configuration Settings

Intercom Route Partition Configuration Settings Description Field Information Is Incorrect

The Intercom Route Partition Configuration Settings description field in the "Configuring Intercom" chapter of the *Cisco Unified Communications Manager Administration Guide* omits a complete list of the non-alphanumeric characters that are not allowed in the description. The unacceptable characters comprise double-quotes ("), angle brackets (<>), square bracket ([ ]), ampersand (&), and percentage sign (%).

Valid Characters in Name Field of Role Configuration Window

In the *Cisco Unified Communications Manager Administration Guide*, be aware that the description for the Name field in the Role Configuration window in the "Role Configuration" chapter is incomplete. The complete description follows:

> Enter a name for the role. Roles can comprise up to 128 characters.
>
> Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Directory Number Chapter Includes Incorrect Information on Alerting Name and Display Name Fields

The "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly describes the Alerting Name field. In addition, The chapter does not describe the relationship between the Alerting Name field and Display (Internal Caller ID) field.

Incorrect Information

For the Alerting Name field, enter a name that you want to display on the phone of the caller.

This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks:

- Forwards the name of the caller that is assigned to the directory number.

- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration.

If you do not configure an alerting name, "Name Not Available" may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field.

Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.

Correct Information

For the Alerting Name field, enter a name that you want to display on the phone of the caller when the called phone is ringing.

This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. When the phone rings at the terminating PINX, if you configured an alerting name for a directory number with shared-line appearances, the system performs the following tasks:

- Forwards the alerting name of the called party, if configured, to the caller.
- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist)

Depending on the state of the call and your configuration, the alerting name, directory number, or display (internal caller ID) configuration may display on the phone, as described in the following bullets.

- Alerting state—The alerting name displays, as configured in the Directory Number window.
- Connected state—If you configure the Display (Internal Caller ID) and the Alerting Name fields, the display (internal caller ID) name displays.
- Connected State—If you configured the Alerting Name field but not the Display (Internal Caller ID) field, the directory number displays.

Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the original dialed number and the alerting name displays during the call.

End User Chapter Includes Incorrect Information for Manager User ID Field

The "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly describes the Manager User ID field.

Incorrect Description

For the Manager User ID field, enter the user ID of the end user manager ID. The manager user ID that you enter must already exist in the directory as an end user.

Correct Description

For the Manager User ID field, enter the user ID of the end user manager ID. The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Cisco Unified Communications Manager does not require that you enter a user ID that already exists in the database.

Device Pool Configuration Chapter Does Not State That You Can Enter -1 in the Connection Monitor Duration Field

The "Device Pool Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* does not state that, for the Connection Monitor Duration field, you can enter -1 or leave the field blank to use the configuration for the enterprise parameter. When you configure the Connection Monitor Duration field in the Device Pool Configuration window, use the following information:

This setting defines the time that the Cisco Unified IP Phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager.

To use the configuration for the enterprise parameter, you can enter -1 or leave the field blank. The default value for the enterprise parameter equals 120 seconds.

Change this setting if you need to disable the connection monitor or if you want to extend the connection monitor time. The maximum number of seconds that you can enter in the field equals 2592000.

Tip When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter.

Trunk Configuration Chapter Does Not State That You Can Enter Hostname in Destination Address Field

The "Trunk Configuration' chapter in the *Cisco Unified Communications Manager Administration Guide* does not state that you can enter a hostname in the Destination Address field, which supports SIP trunks. Use the following information when you configure the Destination Address field:

The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, a hostname, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked.

For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual-stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.

SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.

For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and check the Destination Address is an SRV Destination Port check box.

If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.

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

The description of the Device Name field on the "Phone Configuration" chapter omits the following note:

Note Ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail upon upgrade to a different release of Cisco Unified Communications Manager. If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters.

Recording Destination Address Field Description

In the "Recording Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*, the description of the Recording Destination Address field on the Recording Profile Configuration window omits the following information:

This field allows any characters except the following characters: double quotation marks (“), back quote (‘), and space ( ).

Call Stats Check Box Not Available to Enable Voice Quality Metrics

The Call Diagnostics and Voice-Quality Metrics section of the "Phone Features" chapter of the *Cisco Unified Communications Manager System Guide* incorrectly states that you can check the Call Stats check box on the SIP Profile Configuration window to enable voice quality metrics on Cisco Unified IP Phones for SIP.

That check box no longer exists.

Number of Digits Field Description Is Incorrect

The Application Dial Rules Configuration Error Checking section of the "Dial Rules Overview" chapter of the *Cisco Unified Communications Manager System Guide* misstates information about the Number of Digits field.

The correct information follows:

The Number of Digits field supports digits between 1 and 100, as well as the plus sign (+), the asterisk (*), and the number sign (#). Enter the number of digits of the dialed numbers to which you want to apply this application dial rule. You cannot allow this field to be blank for a dial rule.

OpenLDAP Version 2.3.41 Not Listed in LDAP Synchronization Documentation

The "Understanding the Directory" chapter in the *Cisco Unified Communications Manager System Guide* does not state the version of OpenLDAP that is supported for LDAP Synchronization with Cisco Unified Communications Manager Release 7.1(4).

OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database

DirSync allows you to synchronize data from corporate directories to Cisco Unified Communications Manager. Cisco Unified Communications Manager Release 7.1(4) allows synchronization from OpenLDAP 2.3.41 to the Cisco Unified Communications Manager database. In addition, Unified CM 7.1(4) allows synchronization from the following types of directories that were available in previous releases:

- Microsoft Active Directory 2000 and Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- iPlanet Directory Server 5.1

- Sun ONE Directory Server 5.2
- Sun Java System Directory Server 6.0, 6.1, and 6.2

For more information, refer to the "Understanding the Directory" section of the *Cisco Unified Communications Manager System Guide*.

Application Dial Rules Configuration Error Checking Information Is Incorrect

The Application Dial Rules Configuration Error Checking section in the "Dial Rules Overview" chapter of the *Cisco Unified Communications Manager System Guide* contains incomplete or erroneous information. The correct information follows:

The application dial rules perform the following error checking in the Dial Rule Creation section of the Dial Rules Configuration window:

- The Name field must contain at least one character and supports up to 50 alphanumeric characters, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Ensure each application dial rule name is unique.
- The Description field supports up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>)
- The Number Begins With field supports numeric characters (0-9) as well as plus sign (+), asterisk (*), and number sign (#). The length cannot exceed 50 characters.
- The Number of Digits field supports numeric characters (0-9) only. Ensure that the number is equal to or greater than 0 and less than 100. You cannot allow this field to be blank for a dial rule.
- The Remove Digits field supports numeric characters (0-9) only. Ensure that the number is equal to or greater than 0 and less than 100, and the value in this field cannot be more than the value in the Number of Digits field.
- The Prefix With Pattern field supports numeric characters (0-9) as well as plus sign (+), asterisk (*), and number sign (#). The length cannot exceed 50 characters.
- Ensure that dial rules are unique.
- You cannot allow both the Remove Digits field and the Prefix With Pattern field to be blank for a dial rule.

Time-of-Day Routing Chapter Omits Information About Defined Time Periods

The "Time-of-Day Routing" chapter of the *Cisco Unified Communications Manager System Guide* omits the following information.

If you define a time period with a specific date, on that specified date, that period overrides other periods that are defined on a weekly basis.

Example

Consider the following example:

- A time period, afterofficehours, that is defined as 00:00 to 08:00 from Monday to Friday exists.
- A time period, newyearseve, that is defined as 14:00 to 17:00 on December 31st exists.

In this case, on December 31st, the afterofficehours period does not get considered because it gets overridden by the more specific newyearseve period.

Licensing Chapter Does Not State That You Should Use Microsoft Outlook to Receive Licenses

The "Licensing" chapter in the *Cisco Unified Communications Manager System Guide* does not state that Cisco recommends that you use Microsoft Outlook when you receive Cisco Unified Communications Manager licenses.

Voice Mail Chapters Do Not Describe MWI Service Parameter

The voice mail chapters in the *Cisco Unified Communications Manager System Guide* do not describe the Multiple Tenant MWI Modes service parameter. For information on this service parameter, see the "CSCsx96370 Multiple Tenant MWI Modes Service Parameter" section on page 26.

IP Phones That Work With Mobile Connect and Mobile Voice Access

The System Requirements section of the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* includes this information:

> Mobile Connect works with Cisco Unified IP Phones 7906, 7911, 7941/61, 7962/42, 7970/71, 7975 that are running SIP or SCCP.

Replace that sentence with the following information:

> To see which IP phones work with Mobile Connect and Mobile Voice Access, see the applicable Cisco Unifed IP Phone Administration Guide and Cisco Unified IP Phone User Guide.

Updates to the Configuration Checklist for Cisco Extension Mobility

The information below comprises updates to the Configuration Checklist for Cisco Extension Mobility table of the "Cisco Extension Mobility" chapter of the Cisco Unified Communications Manager Features and Services Guide.

Step 5 omits the following information:

To subscribe the device profile to Cisco Extension Mobility, on the Device Profile Configuration Window, from the related links drop-down list (in the upper right corner of the window), choose "Subscribe/Unsubscribe Services" and click **Go**.

Note Subscribe the directory number and the device profile the same Extension Mobility service.

Step 2 updates:

The second bullet specifies:

- Select values for Service Category and Service Type.

The second bullet should specify:

- Select values for Service Category and Service Type.
  - For Service Category select "XML Service".
  - For Service Type, select "Standard IP Phone Service".

Interaction of Single Number Reach and Privacy

The Privacy section of the Remote Destination Profile Configuration Settings table in the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information:

Note You cannot transfer a call from a cell phone to a desk phone if the RDP Privacy is On, and the "Enforce Privacy Setting on Held Calls" service parameter is set to True.

User Hold and Network Hold MOH Audio Source ID Cannot Be Defined Under Device Pool

The Music On Hold Definitions section of the "Music On Hold" chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly states:

If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is Device Pool-based.

As of Cisco Unified Communications Manager 6.x, that sentence should read:

If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is Common Device Configuration-based

How the Number of Client Matter Codes Affect System Start Up Time

The Interactions and Restrictions section of the "Client Matter Codes and Forced Authorization Codes" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information:

Because the number of Client Matter Codes (CMCs) directly impacts the time that is required for Cisco Unified Communications Manager to start up, limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires approximately 1 hour to start up; a system with 1 million CMCs requires approximately 4 hours to start up.

Barge Initiators Cannot Conference In Additional Callers

The Restrictions section of the "Barge and Privacy" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information.

- The barge initiator cannot conference in additional callers.

IPMASecureSysUser Password Change Procedure

The *Cisco Unified Communications Manager Features and Services Guide* omits the following information.

If you change the IPMASecureSysUser password, you must then go to the **IPMASecureSysUser config > CAPF Profile config** window for the profile that was selected on the IPMA Service Parameters window, change the Certificate Operation to "Install/Upgrade," provide the authentication string, and restart the IPMA service.

CSCsy92863 Intercom Route Partition Online Help Is Incorrect

The Intercom Route Partition Configuration Settings description field in the "Configuring Intercom" chapter of the *Cisco Unified Communications Manager Administration Guide* omits a complete list of the non-alphanumeric characters that are not allowed in the description. The unacceptable characters comprise double-quotes ("), angle brackets (<>), square bracket ([ ]), ampersand (&), percentage sign (%).

Mobile Connect Support Restrictions

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following restriction:

The Mobile Connect feature gets supported only for Primary Rate Interface (PRI) public switched telephone network (PSTN) connections.

For SIP trunks, Mobile Connect gets supported via IOS gateways or intercluster trunks.

Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following (final) step in the "Configuring an H.323 Gateway for System Remote Access by Using Hairpinning" procedure:

Step 5 In the Cisco Unified Communications Manager, create a new route pattern to redirect the incoming MVA number to the H.323 gateway that has the vxml script loaded. Ensure that the Incoming CSS of the gateway can access the partition in which the new route pattern gets created.

Enterprise Feature Access Two-Stage Dialing

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following (final) steps in the "Enterprise Feature Access Two-Stage Dialing" procedure:

Step 8 Ensure that the outbound VOIP dial-peer that is used on the gateway for the initial call leg over to the remote destination (mobile phone) has DTMF-relay configuration in it, so the DTMF codes can get passed through to Cisco Unified Communications Manager.

Step 9 Configure dial-peers on the gateway that receives the second-stage inbound call to the Enterprise Feature Access DID, so the call gets forwarded to the Cisco Unified Communications Manager. Ensure that the VOIP dial-peer has the DTMF-relay configuration in it.

Note If a generic dial-peer is already configured to forward the calls to Cisco Unified Communications Manager and is consistent with the EFA DN, you do not need to perform this step. Ensure that the VOIP dial-peer for this call leg also has a configured DTMF-relay command.

Refer to the *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager* for the list of steps that you need to configure Enterprise Feature Access.

Valid Characters in Name Field of Access List Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name field in the Access List Configuration window in the "Cisco Unified Mobility" chapter is incomplete. The complete description follows:

Enter a text name for the access list.

This name can comprise up to 50 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name and Description Fields of Remote Destination Profile Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name and Description fields on the Remote Destination Profile Configuration window in the "Cisco Unified Mobility" chapter is incomplete. The complete descriptions follow.

Name

Enter a text name for the remote destination profile.

This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Description

Enter a text description of the remote destination profile.

This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Filter Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name field in the Geolocation Filter Configuration window in the "Geolocations and Location Conveyance" chapter is incomplete. The complete description follows:

Enter a unique name for this geolocation filter. Default name cannot be blank.

This field can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, the description for the Name field in the Geolocation Configuration window in the "Geolocations and Location Conveyance" chapter is incomplete. The complete description follows:

Enter a unique name for this geolocation.

The name can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

IPv6 Chapter Incorrectly Describes How IPv6 Addresses Display in the Find and List Phones Window

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly describes how the IP address displays for an IPv6 Only phone in the Find and List Phones window in Cisco Unified Communications Manager Administration.

Incorrect Information

After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window; for phones that have an IPv6 address only, the IPv6 address displays in the window.

Correct Information

After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window. For phones with an IPv6 address only, the IP Address displays as 0.0.0.0 in the IP Address column in the Find and List Phones window. To identify the IPv6 address for the phone, click the **Device Name** link in the Find and List Phones window, which causes the Phone Configuration window to display. For the IPv6 Only device, the Phone Configuration window displays an IPv4 address of 0.0.0.0, listed as IP Address, above the IPv6 address.

Intercom Calls Cannot Be Placed on Hold

The Restrictions section of the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly indicates that intercom calls can be placed on hold. Actually, the system does not allow intercom calls to be placed on hold.

IPv6 Chapter Does Not Contain Information on NTP Server

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not contain the following information on NTP Servers and IPv6.

To avoid potential compatibility, accuracy, and network jitter problems, ensure that the external NTP servers that you specify for the primary node are NTP v4 (version 4). If you are using IPv6 addressing, ensure that the external NTP servers are NTP v4.

Cisco Unified Communications Manager Does Not Support Logical Partitioning for Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express Calls

Cisco Unified Communications Manager does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

The following document omits this limitation:

- book: *Cisco Unified Communications Manager Features and Services Guide, Release 7.1(2)*
  chapter: Logical Partitioning
  topic: Limitations

Mobile Voice Access Directory Number Field Description

In the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide*, the description of the Mobile Voice Access Directory Number field on the Mobile Voice Access window omits the following information:

Enter a value between 1 and 24 digits in length. You may use the following characters: 0 to 9.

Cisco Unified Serviceability

This section contains information on documentation omissions, errors, and updates for Cisco Unified Serviceability.

Password Description Omitted

The Application Billing Server Parameter Settings table in "Configuring CDR Repository Manager" chapter of the *Cisco Unified Serviceability Administration Guide* omits this information:

Password - Enter the password that is used to access the application billing server.

Cluster Service Activation Node Recommendations

The "Configuring Services" chapter in the *Cisco Unified Serviceability Administration Guide* does not include the following information that describes service activation recommendations for specific nodes in a cluster. Table 13 provides a general summary of the cluster activation recommendations for a feature service in these nodes: publisher, subscriber, TFTP, and MOH. For specific recommendations that are associated with activating a particular feature service, refer to the Cluster Service Activation Recommendations section in the "Configuring Services" chapter.

Table 13 Cluster Service Activation Node Recommendations

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager	Deactivated	**Activated**	Deactivated	Deactivated	
Cisco TFTP	Deactivated	Deactivated	**Activated**	Deactivated	
Cisco Messaging Interface	Deactivated	Deactivated	Deactivated	Deactivated	Do not activate this service if you plan to use Cisco Unity voice-messaging system.
Cisco Unified Mobile Voice Access Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use this application, activate this service on the first node only.
Cisco IP Voice Media Streaming App	Deactivated	Deactivated	Deactivated	**Activated**	Do not activate this service on the first node or on any nodes that run the Cisco CallManager service.

Table 13 Cluster Service Activation Node Recommendations (continued)

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CTIManager	Deactivated	**Activated**	Deactivated	Deactivated	Activate this service on each subscriber node to which JTAPI/TAPI applications will connect.
Cisco Extension Mobility	Deactivated	**Optional**	Deactivated	Deactivated	If you use EM, activate this service on all subscriber nodes in the cluster.
Cisco Extended Functions	Deactivated	**Optional**	Deactivated	Deactivated	If you use extended functions, activate this service on one or more servers.
Cisco Dialed Number Analyzer	Deactivated	**Optional**	Deactivated	Deactivated	If you need DHCP service, activate this service on the node with the least amount of call-processing activity.
Cisco DHCP Monitor Service	Deactivated	Deactivated	Deactivated	Deactivated	Activate this service on the node that has DHCP enabled.
Cisco CallManager Attendant Console Server	Deactivated	**Optional**	Deactivated	Deactivated	To use Cisco Unified Communications Manager Attendant Console, activate this service on every subscriber node in the cluster that runs the Cisco CallManager service.
Cisco IP Manager Assistant	Deactivated	**Optional**	Deactivated	Deactivated	If you use IPMA, activate this service on any subscriber nodes (primary and backup - up to six servers for three pairs maximum) in the cluster.
Cisco Web Dialer Web Service	Deactivated	**Optional**	Deactivated	Deactivated	If you use Web Dialer, activate this service on one or more subscriber node(s).
Cisco SOAP-CDRonDemand Service	**Optional**	Deactivated	Deactivated	Deactivated	If you want to collect CDR files by using SOAP, activate the service on the first node only.
Cisco CAR Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAR, activate this service on the first node only.
Cisco AXL Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you need this service, activate the service on the first node only.
Cisco Bulk Provisioning Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use BAT, activate the service on the first node only.
Cisco TAPS Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use TAPS, activate the service on the first node only.
Cisco Serviceability Reporter	**Activated**	Deactivated	Deactivated	Deactivated	Activate this service on the first node only.

Table 13 Cluster Service Activation Node Recommendations (continued)

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager SNMP Service	**Activated**	**Activated**	**Activated**	**Activated**	If you use SNMP, activate this service on all servers in the cluster (optional, but activation recommended).
Cisco CTL Provider	**Optional**	**Optional**	**Optional**	**Optional**	If you use CTL, activate this service on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAPF, activate this service on the first node only.
Cisco DirSync	**Optional**	Deactivated	Deactivated	Deactivated	If you use DirSync, activate this service on the first node only.

Activated = activated at installation

Optional = activate only if the application is needed

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 using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.