



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

February 29, 2012



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).

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:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading to Cisco Unified Communications Manager 7.1\(5\), page 4](#)
- [Service Updates, page 13](#)
- [Related Documentation, page 13](#)
- [Important Notes, page 14](#)
- [New and Changed Information, page 36](#)
- [Caveats, page 55](#)
- [Documentation Updates, page 58](#)
- [Obtaining Documentation and Submitting a Service Request, page 58](#)



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

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 1](#), 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 1 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
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, page 4](#)
- [Special Upgrade Information, page 4](#)
- [Upgrade Paths to Cisco Unified Communications Manager 7.1\(5\), page 8](#)
- [Ordering the Upgrade Media, page 8](#)
- [Service Updates, page 13](#)
- [Upgrading from Cisco Unified Communications Manager Release 5.1\(3e\) to 7.1\(x\) Releases, page 9](#)
- [Upgrading to Unified CM 7.1\(5\) by Using the UCSInstall File, page 9](#)

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 4](#).

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\(5\), page 4](#)
- [I/O Throttling, page 5](#)
- [Write-Cache, page 5](#)
- [Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1\(5\) Upgrade, page 7](#)
- [Making Configuration Changes During an Upgrade, page 7](#)

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 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&treeMdfld>

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).

- [Limitations to Call Park Feature, page 15](#)
- [CSCth53322 Rebuild Server After You Use the Recovery Disk, page 16](#)
- [Verify IPv6 Networking on Servers Before Upgrade, page 16](#)
- [CSCte67180 Wrong Frequency Parameters in Database After an Upgrade Causes Failure, page 17](#)
- [CSCte05285 IBM I3 Servers Automatic Server Restart \(ASR\) Default Specifies Disabled, page 17](#)
- [CSCtf15332 Node Licenses Missing After an Upgrade, page 17](#)
- [CSCtd01766 Destination Port on Trunk Remains Unchanged After Upgrade, page 18](#)
- [CSCte56322 Netscape Browser is not Supported, page 18](#)
- [CSCtd87058 BAT Impact, page 18](#)
- [Unified CM 7.x IOS Device Does Not Offer Full NAT Support for SCCP Version 17, page 18](#)
- [CSCtc99413 Upgrade to Unified CM 7.1\(3x\) from Unified CM 5.x Results in Low Active Partition Disk Alerts, page 18](#)
- [Disaster Recovery System Caution, page 19](#)
- [CSCtb95488 Phones That Support Monitoring and Recording Features, page 20](#)
- [LogCollectionPort Service: selectLogFiles Operation, page 21](#)
- [Perform DRS Backup After You Regenerate Certificates, page 25](#)
- [Important Information About Create File Format Capability in BAT, page 25](#)
- [Limitation Between QSIG PRI and SIP Trunk for MWI, page 25](#)
- [Cisco Unified Communications Manager Assistant Wizard Constraint, page 26](#)
- [Creating a Custom Help Desk Role and Custom Help Desk User Group, page 26](#)
- [Do Not Unplug a USB Device While It Is In Use, page 27](#)
- [Removing Hard Drives, page 27](#)
- [CSCsx96370 Multiple Tenant MWI Modes Service Parameter, page 27](#)
- [Considerations for LDAP Port Configuration, page 28](#)
- [Configuring the Hostname/IP Address for the Cisco Unified Communications Manager Server, page 28](#)
- [SFTP Server Products, page 30](#)
- [SFTP Server Products, page 30](#)
- [Important Information About Delete Transaction by Using Custom File in BAT, page 30](#)
- [TAPS Name Change in Bulk Administration Tool, page 31](#)
- [Basic Uninterruptible Power Supply \(UPS\) Integration, page 31](#)
- [Strict Version Checking, page 31](#)
- [Serviceability Not Always Accessible from OS Administration, page 32](#)
- [Voice Mailbox Mask Interacts with Diversion Header, page 32](#)
- [Best Practices for Assigning Roles to Serviceability Administrators, page 32](#)

- [For Serviceability, the Administrator That Is Created During Installation Must Not Be Removed, page 32](#)
- [Connecting to Third-Party Voice Messaging Systems, page 33](#)
- [Database Replication When You Revert to an Older Product Release, page 33](#)
- [User Account Control Pop-up Window Displays During Installation of RTMT, page 33](#)
- [CiscoTSP Limitations on Windows Vista Platform, page 33](#)
- [Time Required for Disk Mirroring, page 33](#)
- [Changes to Cisco Extension Mobility After Upgrade, page 34](#)
- [RTMT Requirement When Cisco Unified Communications Manager Is Upgraded, page 34](#)
- [Serviceability Session Timeout Is Not Graceful, page 34](#)
- [Serviceability Limitations When You Modify the IP Address, page 34](#)
- [CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value, page 35](#)
- [CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters, page 35](#)
- [CSCtr84167 Block Offnet to Offnet Transfer, page 35](#)
- [CSCtr21486 Troubleshooting Guide Update to Switch Version, page 35](#)
- [MDCX Sendonly Message Suppressed for MGCP Calls, page 35](#)
- [DTMF Suppressed when G.Clear is Advertised, page 35](#)
- [CSCtx00678 Do not use Voicemail for Alerting Name or ASCII Alerting Name, page 36](#)

Limitations to Call Park Feature

The Call Park feature has the following known limitations:

- [CSCsz18443 Cisco Unified IP Phone 8961, 9951, 9971 Registered to a Node may Use the Call Park Number Assigned to Another Node, page 15](#)
- [CSCsz31137 Parked Call Gets Reverted When the Parkee is on, page 16](#)
- [CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve, page 16](#)
- [CSCtb53159 Display Limitation in ConfList, page 16](#)

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

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

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

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

**Note**

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

CSCsz31137 Parked Call Gets Reverted When the Parkee is on

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

CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve

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

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

CSCtb53159 Display Limitation in ConfList

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

CSCth53322 Rebuild Server After You Use the Recovery Disk

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

**Note**

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

Verify IPv6 Networking on Servers Before Upgrade

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

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"/>
              <SetOfFile 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>
              </SetOfFile>
            </item>
          </ServiceList>
        </Node>
      </FileSelectionResult>
    </ns1:SelectLogFilesResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

```

</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_ailed_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 cClearType =
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 2](#) 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 2](#), 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 2 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
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 <i>hostname</i> 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 2](#), 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://sshtwindows.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 3 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 CSCs157629 and CSCs157655 also document this behavior.

For information about the **utils dbreplication clusterreset**, **utils dbreplication dropadmindb**, and **utils dbreplication forcedatasynsub** commands, see the *Command Line Interface Reference Guide for Cisco Unified 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.

CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value

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

CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters

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

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

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

CSCtr84167 Block Offnet to Offnet Transfer

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

CSCtr21486 Troubleshooting Guide Update to Switch Version

When there is a version mismatch between a subscriber server and publisher server, the Cisco Unified Communications Manager history file does not log a switch version entry.

MDCX Sendonly Message Suppressed for MGCP Calls

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

DTMF Suppressed when G.Clear is Advertised

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

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

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

CSCtx86215 Database Replication

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

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

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](#), page 36
- [Cisco Unified Communications Manager Administration](#), page 38
- [Cisco Unified Communications Manager Features and Applications](#), page 40
- [Security](#), page 51
- [Bulk Administration Tool](#), page 53
- [Cisco Unified IP Phones](#), page 53
- [Cisco Unified Serviceability](#), page 54

Command Line Interface

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

Commands Added

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

- [utils ldap config fqdn](#), page 37
- [utils ldap config ipaddr](#), page 37

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 Unified Communications Solutions, Release 7.1(5)*:

- [set network domain, page 37](#)

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 38](#)
- [Menu Changes, page 39](#)
- [Cisco Unified Communications Manager Features and Applications, page 40](#)

New and Updated Enterprise and System Parameters

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

- [Enterprise Parameters, page 38](#)
- [Service Parameters, page 38](#)

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, page 39](#)
- [System, page 39](#)
- [Call Routing, page 39](#)
- [Media Resources, page 39](#)
- [Voice Mail, page 39](#)
- [Device, page 40](#)
- [Application, page 40](#)
- [User Management, page 40](#)
- [Bulk Administration, page 40](#)

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 38](#).

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 \(SIP\), page 40](#)
- [Midcall Codec Support, page 42](#)
- [Unrestricted Export Support, page 45](#)
- [Universal IOS Transcoding, page 45](#)
- [Cisco Mobile 8.0 Support, page 47](#)
- [In-Service Upgrade Enhancements for Cisco Unified IP Phones 8961, 9951, and 9971, page 47](#)

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 4](#).
- 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 5](#).
- Step 13** Click **Save**.

Table 4 *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 5 *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 6](#).
- 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 7](#).
- Step 13** Click **Save**.

Table 6 *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 7 *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 8](#) describes the fields in the **Dual Bank Information** area.

Table 8 *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.

- 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

- In Cisco Unified CM Administration, choose **Device > Device Defaults**.
Check the load information in the **Inactive Load Information** field.
- From the **Bulk Administration > Import/Export > Export > Device Defaults** window, schedule an export job.
- Download the exported tar file.
- Untar the file and check the file format in the exported csv file.
- 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

- Upload the exported tar file to Cisco Unified CM.
- From the **Bulk Administration > Import/Export > Import** window, select the file to upload from the drop-down list.
- Check the override check box and schedule an Import Job.
- In Cisco Unified CM Administration, choose **Bulk Administration > Job Scheduler** window, check the job status.
- 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 52](#).

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 53](#)

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 53](#)

Assisted Directed Call Park on TNP devices

The Assisted Directed Call Park feature enables users to park a call by pressing only one button using the Direct Park feature. This requires administrators to configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.

This feature is supported on the following Cisco Unified IP Phones (SIP) for Cisco Unified Communications Manager 7.1(5) and later:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 9971G

- Cisco Unified IP Phone 9951G
- Cisco Unified IP Phone 8961G

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, page 54](#)

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 57 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 57 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 55.

**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 9 *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 SdITcpConnection, Null PID in TcpStopSessionInd.
CSCtf57240	cp-mediacontrol	IPv6: CUVA(ds) receives a reorder when calling over v6-SIP ICT.
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.

Table 9 Open Caveats for Cisco Unified Communications Manager Release 7.1(5) as of April 10, 2010

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

Documentation Updates

The *Updates to Cisco Unified Communications Manager 7.1(x) Documentation* document provides information about documentation omissions, errors, or updates that are not included in the documentation that supports the Unified CM 8.0(x) release train. To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/7_1_1/71x_cucm_doc-updates.html

Obtaining Documentation and Submitting a Service Request

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)