Release Notes for Cisco Unified Communications Manager Release 7.1(3)

Published September 24, 2009

This document contains information pertinent to Cisco Unified Communications Manager Release 7.1(3).

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.

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the "Important Notes" section on page 10 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(3).

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the "The Latest Software Upgrades for Unified CM 7.1 on Cisco.com" section on page 10.

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

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.

Cisco Unified Communications Manager Business Edition (Unified CMBE) offers you the features and functionality of Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection on one appliance platform.

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(3).

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(3). 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 Business Edition server to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

When Cisco Unified Communications Manager Business Edition 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.

utils system shutdown

Table 1 Supported Servers for Basic Integration

HP Servers	IBM Servers
MCS-7828-H3	MCS-7828-I3
MCS-7828-H4	MCS-7828-I4
	MCS-7828-I4

Upgrading to Cisco Unified Communications Manager 7.1(3)

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

- Before You Begin, page 3
- Special Upgrade Information, page 3
- Upgrade Paths to Cisco Unified Communications Manager 7.1(3), page 8
- Ordering the Upgrade Media, page 8
- The Latest Software Upgrades for Unified CM 7.1 on Cisco.com, page 10
- Upgrading from Cisco Unified Communications Manager Release 5.1(3e) to 7.1(x) Releases, page 8
- Upgrading to Unified CM 7.1(3) by Using the UCSInstall File, page 9
- Upgrading to Unified CM 7.1(3) 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 that, open Cisco Unified Communications Manager Administration. The following information displays:

   – Cisco Unified Communications Manager System version

   – Cisco Unified Communications Manager Administration version

2. Read the "Special Upgrade Information" section on page 3.

Special Upgrade Information

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

- I/O Throttling, page 4

- Write-Cache, page 4
- Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(3) Upgrade, page 6
- Important Upgrade Information, page 6
- Making Configuration Changes After an Upgrade, page 6

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 other MCS-7828 servers. To verify write-cache status, access the 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 was 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 was dead or missing, it would indicate “0”.

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

```
-------------------------------
RAID Details      :

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

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

```
----------
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(3) Upgrade

Before you upgrade to Cisco Unified Communications Manager 7.1(3), 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(3) 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.

Important Upgrade Information

Do not upgrade Cisco Unified CMBE at the same time that the Cisco Unity Connection task Upgrade Database Statistics is running. Because both processes are processor intensive, allowing them to run simultaneously may cause the system to stop functioning and force you to restart the server.

By default, the Upgrade Database Statistics task runs at 3:30 am daily. To determine whether the task schedule has been changed, whether the task is currently running, and how long the task has recently taken to complete, log on to Cisco Unity Connection Administration. Click **Tools > Task Management > Update Database Statistics**.

The Task Definition Basics window displays a history of when the task started and when it completed. If the Time Started column has a value and the Time Completed column does not, this indicates that the task is currently running.

If you must run the upgrade at a time that could overlap with the Upgrade Database Statistics task, reschedule the task to run before or after the upgrade. On the Task Definition Basics window for the task, click **Edit > Task Schedule**.

Do not reschedule the task to run during normal business hours. When the upgrade completes, reset the schedule to the default settings.

Making Configuration Changes After 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, Cisco Unified Serviceability, and the User Option 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, 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 Chapter 7, “Software Upgrades”, 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 is functioning between the first node and the subsequent nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified CM Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Cisco Unified 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 Cisco Unified Real-Time Monitoring Tool, see the *Cisco Unified Cisco Unified Real-Time Monitoring Tool Administration Guide*.

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

Upgrade Paths to Cisco Unified Communications Manager 7.1(3)

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

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

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

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

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

Upgrading from Cisco Unified Communications Manager Release 5.1(3e) to 7.1(x) Releases

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

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

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

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

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

Note During an upgrade from a compatible Cisco Unified CM 5.1 version (see the Compatibility Matrix at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html) to Cisco Unified CM 7.1(3) 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(3) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_7.1.3.10000-11.sgn.iso, comprises two parts:

- UCSInstall_UCOS_7.1.3.10000-11.sgn.iso_part1of2
- UCSInstall_UCOS_7.1.3.10000-11.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_7.1.3.10000-11 build is a nonbootable ISO, it proves useful only for upgrades. You cannot use it for new installations.

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

```
cat UCSInstall_UCOS_7.1.3.10000-11.sgn.iso_part1of2 UCSInstall_UCOS_7.1.3.10000-11.sgn.iso_part2of2 > UCSInstall_UCOS_7.1.3.10000-11.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_7.1.3.10000-11.sgn.iso_part1of2+UCSInstall_UCOS_7.1.3.10000-11.sgn.iso_part2of2 UCSInstall_UCOS_7.1.3.10000-11.sgn.iso
```

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

ebb34e2f516e7a722352ca6b3dd7f922 UCSInstall_UCOS_7.1.3.10000-11.sgn.iso

Step 4 Create a nonbootable DVD that contains the files that are necessary for the upgrade.

Consider the following information:

- Choose the option to burn a disc image, not the option to copy files. Burning a disc image extracts the thousands of files from the .iso file that you created and writes them to a DVD, which is necessary for the files to be accessible for the upgrade.
- Use the Joliet file system, which accommodates filenames up to 64 characters long.
- If the disc-burning application that you use includes an option to verify the contents of the burned disc, choose that option. The application then compares the contents of the burned disc to the source files.

Step 5 Delete unnecessary files, including the two .iso files that you downloaded and the combined .iso file that you created, from the hard disk to free disk space.

The Latest Software Upgrades for Unified CM 7.1 on Cisco.com

You can access the latest software upgrades for Unified CM 7.1 from http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Related Documentation

The view documentation that supports Cisco Unified CM Release 7.1(3), 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(3) 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(3). 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 for Cisco Unified Communications Manager Release 7.1(3).

- HP SCSI Hard Drive Firmware Update, page 11
- CSCtb95488 Phones That Support Monitoring and Recording Features, page 13
- LogCollectionPort Service: selectLogFiles Operation, page 14
- Perform DRS Backup After You Regenerate Certificates, page 18
- Important Information About Create File Format Capability in BAT, page 18
- Limitation Between QSIG PRI and SIP Trunk for MWI, page 18

HP SCSI Hard Drive Firmware Update

The HP SCSI hard drive firmware update issue addresses the following defects:

- CSCse71185: Certain HP Ultra320 SCSI HDs May Exhibit Reduced Perf and Timeouts
- CSCse71295: HP FW Recommended to Min Potential for Media Errors on Certain SCSI HD
- CSCso98836: HP Ultra320 SCSI HDD FW Upgradeh

CSCse71185: Certain HP Ultra320 SCSI HDs May Exhibit Reduced Perf and Timeouts

A ProLiant server configured with any of the HP Ultra320 SCSI hard drives listed in HP Customer Advisory **#C00677430** (available at http://www.hp.com) may exhibit reduced performance or experience excessive timeouts.The dynamically adjusted seek time profile table in the drive firmware causes this performance issue after it becomes degraded.

When this problem occurs, occasional brief delays in command response time while servicing random workloads causes reduced performance and in severe cases the drive may exhibit command timeouts, which require a server reboot for recovery.

CSCse71295: HP FW Recommended to Min Potential for Media Errors on Certain SCSI HD

A ProLiant server configured with any of the HP Ultra320 SCSI hard drives listed in HP Customer Advisory **#C00542020** (available at http://www.hp.com) may report media errors or illuminate the drive fault LED. The corrected firmware version (HPB4 or later) reduces the hard drive idle time that could potentially lead to build-up of media lubricant on the disk surface or drive head, causing the drives to report media errors or illuminate the drive fault LED.

CSCso98836: HP Ultra320 SCSI HDD FW Upgrade

A ProLiant server 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 affected hard drives for these problems are listed in the associated HP Customer Advisories. However, the Cisco provided HP SCSI Hard Drive Firmware Update CD can be applied to all listed server types and the impacted drives will be 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.

The ISO image for the Cisco provided HP SCSI Hard Drive Firmware Update CD and associated readme file may be obtained from Cisco.com at the following navigation path:

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

From the Tools and Resources Downloads 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 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 is

```
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 as those returned by the listNodeServiceLogs operation 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:
  - DownloadtoClient
  - PushtoSFTPServer

  If you select PushtoSFTPServer, then 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:
  - OnDemand
  - Daily
  - Weekly

  - Monthly

Note Only OnDemand option is currently supported for Frequency element. The other options (Daily, Weekly, and Monthly) are applicable for schedule collection that 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 absoulte or relative. If you prefer relative time range, then 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 is 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 avilable options are:
  - True—The files are compressed.
  - False—The files are not compressed.

  RemoteFolder—The remote folder where the files are to be uploaded. This option is used only if you choose to upload trace files to SFTP or FTP server.

Request Example

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:SelectLogFiles soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
   <FileSelectionCriteria href="#id0"/>
  </ns1:SelectLogFiles>
  <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:SchemaFileSelectionCriteria"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
   <ServiceLogs xsi:type="soapenc:Array" soapenc:arrayType="xsd:string[45]">
    <item>Cisco Syslog Agent</item>
    <item>Event Viewer-Application Log</item>
    <item>Install Logs</item>
    <item>Event Viewer-System Log</item>
    <item>Security Logs</item>
   </ServiceLogs>

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

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

Response Example

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

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:SelectLogFilesResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
<FileSelectionResult xsi:type="ns2:SchemaFileSelectionResult"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
<Node xsi:type="ns2:Node">
<name xsi:type="xsd:string">MCS-SD4</name>
<ServiceList soapenc:arrayType="ns2:ServiceLogs[1]" xsi:type="soapenc:Array"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<item xsi:type="ns2:ServiceLogs">
<name xsi:type="xsd:string" xsi:nil="true"/>
<SetOfFiles soapenc:arrayType="ns2:file[5]" xsi:type="soapenc:Array">
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000305.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000305.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097082</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 04:14:05 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000306.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000306.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097083</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 05:41:26 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000307.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000307.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096868</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 07:08:56 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000308.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000308.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096838</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:36:17 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000309.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000309.txt</absolu
tepath>
<filesize xsi:type="xsd:string">100657</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:40:20 PST 2009</modifiedDate>
</item>
</SetOfFiles>
</item>
</ServiceList>
</Node>
</FileSelectionResult>
<ScheduleList soapenc:arrayType="ns3:Schedule[0]" xsi:type="soapenc:Array"
xmlns:ns3="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"/>
</ns1:SelectLogFilesResponse>
</soapenv:Body>
```

```
</soapenv:Envelope>
```

Fault

If the specified frequency is null, it will throw 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 only 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 a SsDataInd signal while in the mwi_nailed_up_ssinfores state, MessageWaiting will not process any subsequent MWIs.

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

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

Cisco Unified Communications Manager Assistant Wizard Constraint

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

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

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

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

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

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

Step 2 Click **Add New**.

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

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

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

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

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

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

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

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

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

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

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

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

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

Next Steps

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

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

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

Do Not Unplug a USB Device While It Is In Use

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

Removing Hard Drives

Cisco only supports replacing failed hard drives. Cisco does not support drive pulling/swapping as a method of fast upgrade reversion, restore, or server recovery.

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. 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(3).

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 bullets. 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.)

Adding or Updating SIP Dial Rules Causes Cisco TFTP Service to Rebuild All Phone Configuration Files

When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule.

CSCta10219 Unicast Music on Hold May Not Play

After you invoke music on hold (MOH) several times, unicast MOH may not play. You can invoke MOH by using hold, transfer, conference, park, and so on.

The unicast MOH may resume playing on later hold attempts

Workaround - Option 1

Upgrade to a version of Cisco Unified Communications Manager that contains a fix for this issue.

Workaround - Option 2

Configure the MOH servers to send out multicast MOH and unicast MOH on the same MOH resources.

Procedure

Step 1 Configure each MOH audio source ID for multicast.

Step 2 Configure each MOH server to multicast.

Step 3 Make sure that Media Resource Groups (if any are defined) do not have multicast enabled.

Be aware that no network (router) changes to forward multicast MOH packets are required if Media Resource Groups (MRG) are not configured to enable multicast MOH.

Note The MOH servers transmit multicast streams for each MOH source and MOH codec, so network traffic to the local network may increase. The multicast streams will remain continuous and run at all times.

The MOH servers send the multicast streams to the local router; but, if the rounter is not configured to forward the MOH multicast packets, impact to the LAN traffic will be minimal. By default, routers do not forward multicast MOH packets.

Alerts During Upgrades to Cisco Unified Communications Manager Business Edition 6.1(4)

During an upgrade to Cisco Unified Communications Manager Business Edition, users may experience following alerts in the Cisco Unified Real-Time Monitoring Tool. Users may disregard these alerts during the upgrade process:

- NumberOfRegisteredPhonesDropped
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredGatewayDecreased
- NumberOfRegisteredGatewayIncreased

SFTP Server Products

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

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

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

CSCsu08609 Blind Transfer or Unanswered Conference Call over QSIG PRI Trunk

A blind transfer or an unanswered conference call that gets forwarded to voice-mail over QSIG PRI trunk reaches the general greeting instead of the called party.

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 6.1(4) 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 will commence as soon as the low battery threshold is reached. Resumption or fluctuation of power will 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:

Restore Examples

From version	To version	Allowed / Not allowed
7.1(2).1000-1	7.1(3).1000-1	Not allowed
7.1(3).1000-1	7.1(3).1000-2	Not allowed
7.1(3).1000-1	7.1(3).2000-1	Not allowed
7.1(3).1000-1	7.1(3).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 the voice-messaging system has a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager Release 5.0 or later, use a Cisco certified serial-to-USB adapter with the part number USB-SERIAL-CA=.

Database Replication When You Revert to an Older Product Release

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

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

For information about the utils **dbreplication clusterreset**, **utils dbreplication dropadmindb**, and **utils dbreplication forcedatasyncsub** commands, see the *Command Line Interface Reference Guide for Cisco Unified 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.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 3 hours.

Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 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 making 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 & 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. When you modify the IP Address field, you will need to re-create the RTMT profile, custom counters, custom alerts, and generic queries for TLC the next time that you log in to the server on RTMT.

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

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

New and Changed Information

This section contains information on the following topics:

Installation, Upgrade, and Migration

This section contains information on the following topics:

Enabling Write-Back Cache for Improved Upgrade Performance

If you upgrade from Cisco Unified Communications Manager Release 7.1(3) to a later release in the future, the following warning will display when you start the upgrade if your server write-back cache is disabled. The warning requires you to approve this information before you continue your upgrade:

> **Warning:** The hard disk controller write-back cache is disabled. To enable the cache, replace the disk controller battery. After the new battery charges fully, the write-back cache enables automatically. If you run an upgrade with a disabled write-back cache, you will slow the upgrade process and cause call processing failures.
>
> If you replaced the battery, use the Show Hardware menu on the OS Administration windows to see the battery recharge status.

Maintaining Correct Time Zone Data

To ensure that Cisco Unified Communications Manager Release 7.1(3) includes the latest time zone information, you can install a COP file that updates the time zone information after you install Cisco Unified Communications Manager Release 7.1(3). You do not need to upgrade Cisco Unified Communications Manager Release 7.1(3) to get these updates. After major time zone change events, Cisco contacts you to let you know that you can download COP file *ciscocm.dst-updater.YYYYv-1.el4.7.1.3.cop* to install on the server. (In the preceding file name example, "YYYY" represents the release year of the COP file, and "v" specifies the file version number.).

Note Be aware that COP files that contain "7.1.3" in their filenames are compatible with only Release 7.1(3).

For information about how to install a COP file, follow the installation instructions that you get with the file.

Cisco Unified Communications Operating System Administration

This section contains information on the following topics:

- Nonstandard Error Message for Unsupported Upgrades to Cisco Unified Communications Manager Release 7.1(3), page 28

Nonstandard Error Message for Unsupported Upgrades to Cisco Unified Communications Manager Release 7.1(3)

You cannot upgrade directly from Cisco Unified Communications Manager Releases 6.0(1) or 6.1(2) to Release 7.1(3); however, if you attempt this upgrade, the standard error message does not display. Instead, the following error message displays.

errors.upgrade.fromVersionDisallowed

Command Line Interface

The following changes to Command Line Interface commands exist in release 7.1(3)

- Commands Added, page 28
- Commands Removed, page 29

Commands Added

The following commands get added in Cisco Unified Communications Manager 7.1(3).

- **show tech dberrcode**—Displays information (from the database log files) about the error code that is specified.

  Syntax: **show tech dberrcode** [*errorcode*]

- **show tech dumpCSVandXML**—Provides detailed information for customer support in the case of an L2 upgrade condition.

  Syntax: **show tech dumpCSVandXML**

- **show tech repltimeout**—Displays the replication timeout. When it gets increased, it ensures that as many servers as possible in a large system will get included in the first round of replication setup. If you have the maximum number of servers and devices, set the replication timeout to the maximum value. Be aware that this will delay the initial set up of replication (giving a chance for all servers to be ready for setup).

  Syntax: **show tech repltimeout**

- **utils dbreplication dropadmindbforce**—Drops the Informix syscdr database on the serveron which it is run. This command should only be run when requested by customer support.
- **utils dbreplication repairreplicate**—This command repairs mismatched data between cluster nodes and changes the node data to match the publisher data. It does not repair replication setup.

  Syntax:**utils dbreplication repairreplicate replicatename [nodename]|all**

- **utils dbreplication repairtable**—This command repairs mismatched data between cluster nodes; and changes the node. to match the publisher data. It does not repair replication setup.

  Syntax: **utils dbreplication repairtable tablename [nodename]|all**

- **utils reset_application_ui_administrator_password**—Resets the application user interface administrator password.

  Syntax: **utils reset_application_ui_administrator_password**

- **utils reset_application_ui_administrator_name**—Resets the application user interface administrator name.

  Syntax: **utils reset_application_ui_administrator_name**

- **show tech activesql—**Displays the active queries to the database taken at 1-minute intervals as far back as the logs allow.

  Syntax: **show tech activesql**

- **file list license**—New parameter for the file list command that lists the license file that is specified by license.

  Syntax: **file list license** *filename* **[page] [detail] [reverse] [date | size]**

- **file view license**—New parameter for the file view command that displays the license file that is specified by license.

  Syntax: **file view license** *filename* views the license file that is specified by *license*.

- **file get license**—New parameter for the file get command that sends the license file that is specified by license.

  Syntax: **file get license** *filename* [**reltime**] [**abstime**] [**match**] [**recurs**] [**compress**]

Commands Removed

Cisco Unified Communications Manager 7.1(3) removes the following commands.

- **utils system upgrade list**
- **utils system upgrade get**
- **utils system upgrade start**

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

- New and Updated Enterprise and System Parameters, page 30
- Menu Changes, page 30
- Cisco Unified Communications Manager Features and Applications, page 31

New and Updated Enterprise and System Parameters

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

- Enterprise Parameters, page 30
- Service Parameters, page 30

Enterprise Parameters

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

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.

- Dial-via-Office Forward Service Access Number—See the "Cisco Unified Mobility Dial-Via-Office Forward" section on page 33.
- The SIP Interoperability Enabled service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager supports Session Initiation Protocol (SIP) for SIP stations and SIP trunks. Devices that run SIP, for example, phones and trunks, require that you set this parameter to True; when you set this parameter to False, Cisco Unified Communications Manager ignores SIP messages, and SIP devices do not function; that is, phones that run SIP cannot register with Cisco Unified Communications Manager, and SIP trunks cannot interact with Cisco Unified Communications Manager. The default value specifies True. You must restart the Cisco CallManager service if you change the value of this parameter.

Menu Changes

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

- Main Window, page 31
- System, page 31
- Call Routing, page 31
- Media Resources, page 31
- Voice Mail, page 31
- Device, page 31
- Application, page 31
- User Management, page 31

- Bulk Administration, page 31

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 30.

Call Routing

The Call Routing menu contains the following change:

- Call Routing > Directory Number—See the "Create Cisco Unity Voice Mailbox Option Removed from Directory Number Configuration Window" section on page 32.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

The Device menu contains the following updates:

- In some device configuration windows, the Device Is Trusted or Device Is Not Trusted message displays. See the "Security Icon Enabled by Phone Model" section on page 48.
- Device > Device Settings > Feature Control Policy—See the "Feature Control Policy in Cisco Unified Communications Manager Administration" section on page 39.

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. See the "Support for Feature Control Policy" section on page 50.

Cisco Unified Communications Manager Features and Applications

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

- OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database, page 32
- Cisco Unified Communications Manager Assistant Restart, page 32

- Create Cisco Unity Voice Mailbox Option Removed from Directory Number Configuration Window, page 32
- Cisco Unified Mobility Dial-Via-Office Forward, page 33
- DN Capacity Increase for the Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 38
- Enterprise Phone Configuration in Cisco Unified Communications Manager Administration, page 38
- Feature Control Policy in Cisco Unified Communications Manager Administration, page 39
- Logical Partitioning Interaction with Block OffNet to OffNet Transfer Service Parameter, page 39
- Logical Partitioning Policy Tree Construction, page 40
- Logical Partitioning Policy Search Algorithm, page 41
- Redirected Dialed Number Identification Service and Diversion Header, page 42
- SIP Gateway Protocol Supports Mobile Voice Access, page 43
- Support for Microsoft Active Directory Application Mode LDAP Server, page 44

OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database

DirSync allows you to synchronize data from corporate directories to Cisco Unified Communications Manager. Cisco Unified Communications Manager Release 7.1(3) allows synchronization from OpenLDAP 2.3.41 to the Cisco Unified Communications Manager database. In addition, Unified CM 7.1(3) allows synchronization from the following types of directories that were available in previous releases:

- Microsoft Active Directory 2000 and Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- iPlanet Directory Server 5.1
- Sun ONE Directory Server 5.2
- Sun Java System Directory Server 6.0, 6.1, and 6.2

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

Cisco Unified Communications Manager Assistant Restart

In release 6.1(4) and 7.1(3), if the system administrator changes a user username, preferred location, or password (assistants), that user does not get logged off. For user-ID changes, neither the manager nor his or her assistant gets logged off when that manager user ID gets changed; however, an assistant gets logged off the assistant phone and the Assistant Console when that assistant user ID gets changed.

Create Cisco Unity Voice Mailbox Option Removed from Directory Number Configuration Window

In Cisco Unified Communications Manager Business Edition 7.1(3), the Create Cisco Unity Voice Mailbox option in the Related Links drop-down list box no longer displays in the Directory Number Configuration window in Cisco Unified Communications Manager Administration; therefore, you cannot create a Cisco Unity Connection voice mailbox from this window.

The “Directory Number Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition (Release 7.1(2))* and online help incorrectly state that you can create a Cisco Unity Connection voice mailbox from this window.

Cisco Unified Mobility Dial-Via-Office Forward

Release 7.1(3) of Cisco Unified Communications Manager supports the Dial-via-Office Forward (DVO-F) feature as part of the capabilities that Cisco Unified Mobility supports.

Users that have Cisco Mobile, a Cisco Unified Mobile Communicator application, installed on their mobile devices can take advantage of the Dial-via-Office Forward feature. Cisco Unified Mobile Communicator invokes the Dial-via-Office Forward feature from the mobile device through SIP signaling over the data channel between Cisco Unified Mobile Communicator-Cisco Unified Mobility Advantage and Cisco Unified Mobility Advantage-Cisco Unified Communications Manager to initiate calls to a final target. Because the calls are anchored at the enterprise, the feature offers a cost-saving solution to Cisco Unified Mobile Communicator mobile users.

Note Only Cisco Unified Mobile Communicator devices with the Cisco Mobile client can invoke the Dial-via-Office Forward feature.

Cisco Unified Communications Manager returns the Dial-via-Office Forward (DVO-F) service access number, if the DVO-F service access number has been configured, or the Enterprise Feature Access (EFA) directory number (DN) through the data channel. The Cisco Unified Mobile Communicator client that runs on the mobile phone calls the number that it receives from Cisco Unified Communications Manager. The phone number of the mobile device that makes the DVO-F call gets matched against configured Mobility Identities (MI), thus ensuring that the system places only those calls that authorized users make. If a match occurs, the call request gets sent to the target party. Both complete match and partial match get supported, depending on the setting of the Matching Caller ID with Remote Destination service parameter.

This section covers the following topics for the Dial-via-Office Forward feature:

- Configuration of Dial-via-Office Forward in Cisco Unified Communications Manager Administration, page 34
- Dial-via-Office Forward Service Access Number, page 34
- Globalization Support for DVO-F Service Access Number, page 34
- Use Case Scenarios for Dial-via-Office Forward, page 35
- Dial-via-Office Forward Call Characteristics, page 35
- Example of Dial-via-Office Forward, page 36
- SIP Error Codes, page 36
- Dial-via-Office Forward Configuration Tips, page 36
- Dial-via-Office Forward Limitations, page 37
- Enforcement of a Single DVO-F Call per Cisco Unified Mobile Communicator Device, page 37
- Additional Documentation, page 37

Configuration of Dial-via-Office Forward in Cisco Unified Communications Manager Administration

The following configuration must take place in Cisco Unified Communications Manager Administration for the Dial-via-Office Forward feature to be enabled:

- **Call Routing > Mobility Configuration**

  The value of the Enterprise Feature Access Directory Number setting should match the called number and should belong to the correct partition.

- **System > Service Parameters**

  The Dial-via-Office Service Access Number can specify an alternate number.

Dial-via-Office Forward Service Access Number

Release 7.1(3) of Cisco Unified Communications Manager introduces a new service parameter, Dial-via-Office Forward Service Access Number. This service parameter provides customers the option to set up a dedicated number for Cisco Unified Mobile Communicator users to dial DVO-F while Cisco Unified Communications Manager receives the calls on a different number (for example, through 1-800 support). The DVO-F service access number can specify a toll-free 1-800 number, which the service provider can map to a local number that reaches the enterprise or to any other alternative number for Cisco Mobile clients to invoke DVO-F calls.

The Dial-via-Office Forward Service Access Number service parameter has the following characteristics:

- Length specifies up to 24 dialable digits.
- Does not specify a partition.

The Dial-via-Office Service Access Number service parameter interacts with the existing Enterprise Feature Access (EFA) DN as follows:

- At least one of the numbers, either the EFA DN or the DVO-F service access number, must be configured to invoke the DVO-F feature.
- For the 183 Session in progress message response, the following rules apply:

  If the Dial-via-Office Forward Service Access Number service parameter number is configured, Cisco Unified Communications Manager sends this alternative number to Cisco Unified Mobility Advantage in SDP.

  If only EFA DN is configured, Cisco Unified Communications Manager sends the EFA DN to Cisco Unified Mobility Advantage.

- For incoming PSTN calls, the following matching takes place:

  Called party number gets matched against either the EFA DN or the DVO-F Service Access Number. Either Partial Match or Complete Match takes place, depending on the setting of the Matching Caller ID with Remote Destination service parameter.

  If a match is found, the voice call correlates with the previous SIP call, and the Call Await Timer gets stopped.

  If no match is found, after the Call Await Timer expires, the call disconnects, and the 503 Service Unavailable message gets sent.

Globalization Support for DVO-F Service Access Number

The Dial-via-Office Forward Service Access Number supports the following dialable digits:

- 0 through 9
- +, which must be preceded by backslash (\). Because backslash is not a dialable digit, it does not count toward the maximum length of 24 digits.

- * and #
- A through D

The preceding special characters can occur in any position.

Use Case Scenarios for Dial-via-Office Forward

The Dial-via-Office Forward feature supports the following use case scenarios:

1. Enterprise has configured EFA DN only.

   The DVO-F feature succeeds only when the Cisco Unified Mobile Communicator user dials the exact EFA DN and Cisco Unified Communications Manager also receives the identical call party number.

   Example

   EFA DN = 1239876

   DVO-F Service Access Number service parameter = EMPTY

   Cisco Unified Communications Manager sends 1239876 in 183 message and receives PSTN call to 1239876.

2. Enterprise provides a 1-800 toll-free number for DVO-F calls.

   Enterprise sets up a toll-free number, which may be mapped to an actual number (ring-to number) when the service provider receives the call.

   If the ring-to number gets applied, administrator must configure the toll-free number (for example, 18008889999) by using the Dial-via-Office Forward Service Access Number service parameter and the ring-to number (for example, 4081239876) as the EFA DN.

   Example

   EFA DN = 1239876 (localized format, depending on service provider)

   DVO-F Service Access Number service parameter = 18008889999

   Cisco Unified Communications Manager sends 18008889999 in 183 Session in progress message and receives PSTN call to 1239876.

Dial-via-Office Forward Call Characteristics

Using the preceding example, the following characteristics apply to a Dial-via-Office Forward call:

- Based on the INVITE SDP parameter “a=setup:active,” Cisco Unified Communications Manager determines that the Cisco Mobile client wants to initiate a DVO-F call.
- The Call Await Timer, which is set to 30 seconds, starts when Cisco Unified Communications Manager sends the 183 Session In Progress message to Cisco Unified Mobility Advantage.
- If the Cisco Unified Communications Manager does not receive a PSTN call from Cisco Unified Mobile Communicator before the Call Await Timer expires, Cisco Unified Communications Manager sends a “503 Service Unavailable” message and clears resources that are associated with the DVO-F Invite.
- When a PSTN call arrives, the following attempts at matching take place:

  Cisco Unified Communications Manager tries to match the calling party number against known Mobility Identities (MIs) to determine whether the call will get anchored. Cisco Unified Communications Manager performs the match based on the option that is set for the Matching Caller ID with Remote Destination service parameter (either Partial Match or Complete Match).

  Cisco Unified Communications Manager also tries to match the called party number against the EFA DN or DVO-F service access number and determines whether the call is a DVO-F call.

- After the call gets established, the user can invoke other Cisco Unified Mobility features, such as hold, resume, conference, transfer, and desk pickup.

Refer to the "Use Case Scenarios for Dial-via-Office Forward" section on page 35 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Example of Dial-via-Office Forward

The following example illustrates the sequence of events that takes place in an instance of Dial-via-Office Forward (DVO-F):

1. User launches the Cisco Unified Mobile Communicator application and enters 2000 as target number.
2. Cisco Unified Mobile Communicator sends SIP Invite message with target number as 2000.
3. Cisco Unified Communications Manager sends back 183 Session In Progress via the data channel. The SDP parameter specifies the Dial-via-Office Forward service access number or EFA DN.
4. Cisco Unified Mobile Communicator autodials the number that the SDP specifies.
5. Cisco Unified Communications Manager correlates this voice call with the SIP data channel call by comparing the calling party number with the Mobility Identity and by comparing the called party number with the EFA DN or the DVO-F service access number.
6. The call then progresses normally.

SIP Error Codes

Release 7.1(3) of Cisco Unified Communications Manager provides specific SIP error codes when a DVO-F call does not succeed. The following table provides the SIP error codes for unsuccessful DVO-F calls.

Call Scenario	SIP Error Code
Target number is not routable.	404 Not Found
Target is busy.	486 Busy Here
Cisco Unified Mobile Communicator hangs up before target answers.	487 Request Terminated
Cisco Unified Mobile Communicator sends SIP CANCEL.	487 Request Terminated

Dial-via-Office Forward Configuration Tips

The following configuration tips apply when you are configuring the Dial-via-Office Forward feature:

- Cisco Unified Mobile Communicator device must get provisioned with a valid Mobility Identity (MI).
- Cisco Unified Mobile Communicator device must register with Cisco Unified Communications Manager.
- If the Cisco Unified Mobile Communicator caller ID that the Cisco Unified Communications Manager receives does not match the provisioned MI completely, perform the following configuration:

  Set the Matching Caller ID with Remote Destination service parameter to Partial Match.

  Specify the number of matched digits in the Number of Digits for Caller ID Partial Match service parameter.

- Make sure the ingress gateway gets configured properly, so the called party number matches either the EFA DN or the DVO-F Service Access Number service parameter.
- If the called party number is expected to match the EFA DN, ensure that the Inbound Calling Search Space for Remote Destination service parameter is set properly as follows:

  If the Trunk or Gateway Inbound Calling Search Space option is chosen, the EFA DN partition must belong to the trunk or gateway calling search space.

  If the Remote Destination Profile + Line Calling Search Space option is chosen, the EFA DN partition must belong to the calling search spaces of the Cisco Unified Mobile Communicator device and its enterprise DN.

Dial-via-Office Forward Limitations

The Dial-via-Office Forward (DVO-F) feature specifies these limitations in Release 7.1(3) of Cisco Unified Communications Manager:

- DVO-F cannot support simultaneous DVO-F calls from a single Cisco Unified Mobile Communicator device.
- DVO-F relies on caller ID to correlate a PSTN call with the SIP call:

  If the called party number cannot go through the GSM network, the DVO-F call fails. A standard service provider announcement will play. Cisco Unified Communications Manager sends a 503 Service Unavailable message after the Call Await Timer expires.

  If Cisco Unified Communications Manager does not receive the calling party number (that is, the Cisco Unified Mobile Communicator user blocks his or her caller ID), the DVO-F call fails. A reorder tone will play. Cisco Unified Communications Manager sends the 503 Service Unavailable message after the Call Await Timer expires.

Enforcement of a Single DVO-F Call per Cisco Unified Mobile Communicator Device

Release 7.1(3) of Cisco Unified Communications Manager does not support multiple, simultaneous DVO-F calls from a single Cisco Unified Mobile Communicator device.

If a second DVO-F call gets received from the same Cisco Mobile client while the first DVO-F call is in progress with an established voice path, Cisco Unified Communications Manager rejects the second DVO-F call with a SIP 491 “Request Pending” response.

If a second DVO-F call gets received from the same Cisco Mobile client while the first DVO-F call is still in process and before a voice path has been established, Cisco Unified Communications Manager cancels the first DVO-F call with a SIP 487 “Request Terminated” response and processes the second DVO-F call Invite.

Additional Documentation

For more information about configuring the Cisco Unified Mobile Communicator to operate with Cisco Unified Communications Manager, see the following documents:

- “Configuring Cisco Unified Communications Manager for Use With Cisco Unified Mobility Advantage” chapter in *Installing and Configuring Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.
- *Configuring Features in Cisco Unified Mobility Advantage: Dial Via Office Forward* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

DN Capacity Increase for the Cisco Unified IP Phone Expansion Modules 7915 and 7916

The Cisco Unified IP Phone Expansion Modules 7915 and 7916 attach to your Cisco Unified IP Phone 7962G, 7965G, or 7975G, adding up to 48 extra line appearances or programmable buttons to your phone. The line capability increase includes DN, line information menu, line ring menu, and line help ID.

You can configure all the 48 additional keys on the Cisco Unified IP Phone Expansion Modules 7915 and 7916. Access the Phone Button Template Configuration window to configure the buttons.

Cisco Unified Communications Manager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.

To configure the 48 additional buttons, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.

Step 2 Click the **Add New** button.

Step 3 From the drop-down list, choose a template and click **Copy**.

Step 4 Rename the new template.

Step 5 Update the template to 56 Directory Numbers for Cisco Unified IP Phone 7975G, or 54 Directory Numbers for Cisco Unified IP Phones 7965G and 7962G.

Refer to *Cisco Unified Communications Manager Administration Guide* for more information on creating and modifying templates.

Enterprise Phone Configuration in Cisco Unified Communications Manager Administration

Cisco Unified IP Phone firmware release 8.5(2) allows you to disable the Join and Direct Transfer Policy parameter in Cisco Unified Communications Manager Administration in the Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**) for the following phones:

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 696

Because some JTAPI and TAPI applications are not compatible with the join and direct transfer features, for these applications to control and monitor the Cisco Unified IP Phones 6921, 6941, and 6961, you may need to disable join or direct transfer on the same line and, possibly, across lines. Refer to the documentation of the JTAPI or TAPI application(s) that you are running.

Tip Be aware that no other parameters in the Enterprise Phone Configuration window are supported at this time.

Where To Find More Information

- *Cisco Unified IP Phone 6921, 6941, and 6961 Administration Guide for Cisco Unified Communications Manager 7.1 (SCCP)*, “Configuring Features, Templates, Services, and Users” chapter
- *Cisco Unified Communications Manager Administration Guide, Release 7.1(2)*

Feature Control Policy in Cisco Unified Communications Manager Administration

Feature control policy requires additional phone support to work. At this time, if you configure feature control policy, the functionality does not work.

Logical Partitioning Interaction with Block OffNet to OffNet Transfer Service Parameter

Release 7.1(2) of Cisco Unified Communications Manager omitted the interaction of logical partitioning with the Block OffNet to OffNet Transfer service parameter that specifies whether to block offnet-to-offnet call transfers. This interaction now appears in Release 7.1(2) of Cisco Unified Communications Manager and subsequent releases.

The existing Block OffNet to OffNet Transfer service parameter allows the Transfer feature to block the transfer operation when both Transferred and Transferred Destinations specify offnet calls.

Refer to the “Setting the Block OffNet to OffNet Transfer Service Parameter” section in the “External Call Transfer Restrictions” chapter of the *Cisco Unified Communications Manager Features and Services Guide* for more information about this service parameter.

The Cisco Unified Communications Manager system that is disabled for logical partitioning retains the expected behavior that this service parameter specifies.

Logical Partitioning-Enabled System

In a logical partitioning-enabled Cisco Unified Communications Manager system, you can configure the system to allow multiple Voice Gateway (PSTN) participants that use the GeolocationPolicy, GLPolicyX, in a supplementary feature by configuring a policy such as the following one:

GLPolicyX Border GLPolicyX Border Allow

After Cisco Unified Communications Manager configures such a policy, be aware that all features (such as Forwarding, Transfer, Ad Hoc Conference, and so forth) are allowed between participants that use GeolocationPolicy, GLPolicyX Border. For example, forwarding a call that comes from a party that uses GLPolicyX Border to another party that uses GLPolicyX Border gets allowed.

Assume that Cisco Unified Communications Manager deployment requires that all supplementary features except the Transfer feature function for such participants. If so, the Block OffNet to OffNet Transfer service parameter can block transfer between offnet devices even if the logical partitioning policy is allowed.

This service parameter controls only the blocking of offnet-to-offnet transfers and does not impact any other supplementary features. Thus, the following details highlight scenarios that involve voice-gateway-to-voice-gateway transfers.

Details

1. Border-to-Border Logical Partitioning Policy Specifies Deny

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager denies the transfer. The “External Transfer Restricted” message displays to the transferring party.

The Cisco Unified Communications Manager setting (either True or False) for the Block OffNet to OffNet Transfer service parameter does not affect the Transfer operation.

The logical partitioning Deny policy takes precedence, and Cisco Unified Communications Manager follows the policy strictly.

2. Border-to-Border Logical Partitioning Policy Specifies Allow

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager checks the allow policy and also checks the setting of the Block OffNet to OffNet Transfer service parameter. This service parameter thus affects the transfer between offnet participants.

   a. Block OffNet to OffNet Transfer service parameter specifies True—Cisco Unified Communications Manager checks whether both parties (transferred and transferred destination) are offnet. If so, the transfer of such calls gets denied, and the "External Transfer Restricted" message displays to the transferring party.

      Because transfer gets blocked due to the service parameter, the serviceability Perfmon counter for Logical Partitioning Transfer Failures does not increment.

   b. Block OffNet to OffNet Transfer service parameter specifies False—Transfer succeeds.

Offnet/Onnet Behavior for a Device

For outgoing calls, the Call Classification setting in the Route Pattern Configuration window determines the offnet or onnet value. The Call Classification value in the Route Pattern Configuration window overrides the device-level configuration or the corresponding value of the Call Classification service parameter.

For incoming calls, the device-level configuration or the corresponding Call Classification service parameter value determines the offnet or onnet value.

Logical Partitioning Policy Tree Construction

In the *Cisco Unified Communications Manager Features and Services Guide, Release 7.1(2),* the "Logical Partitioning" chapter omits a description of the logical partitioning policy tree construction, which the following text provides. The omitted description will directly follow the figure, "Example Policy Tree for Logical Partitioning Policies for India Cluster," in future editions of the document.

Policy Tree Construction

The policy tree construction follows a fixed algorithm. The policy tree includes a source portion and a target portion.

1. [GLP_X Border GLP_Y Interior] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.
2. [GLP_Y Interior GLP_X Border] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

Thus, the Border-to-Interior policy specifies that the Border part always originates in the source portion of the tree. The policy gets added in a leaf node.

3. [GLP_X Border GLP_Y Border] policy gets added.

First, a determination decides whether to add GLP_X in the source portion or GLP_Y in the source portion.

If no existing policy matches any tokens of GLP_X or GLP_Y (due to other GLP policy), the tree construction takes the source portion from GLP_X Border and the target portion from GLP_Y Border.

If an existing policy matches some tokens in the source portion, the source portion gets taken from that GLP.

Example 1: GLP_Y Border GLP_X Interior is already configured.

Because GLP_Y is already used in the source portion, to add the [GLP_X Border GLP_Y Border] policy, the GLP_Y gets added in the source portion.

Example 2: If the two policies, [GLP_X Border GLP_Y Interior] and [GLP_Y Border GLP_X Interior] exist, two source branches exist that both start with Border.

Assume that GLP_B overlaps more tokens with GLP_X (as compared to GLP_Y) and GLP_A does not match any Border branches.

To add the [GLP_A Border GLP_B Border] policy, the policy gets searched as to whether GLP_A or GLP_B can fit in the existing source branches.

As GLP_B matches some tokens from GLP_X, the portion of the tree gets shared with GLP_X.

Assume that Border:IN:KA:BLR:BLD1 to Border:IN:MH:MUM:BLD1 exists.

Adding Border:IN:MH:Pune:BLD1 to Border:IN:KA:BLR:BLD2 policy uses the source portion of Border:IN:KA:BLR and adds BLD2 in the leaf of the source tree and adds a target portion of Border:IN:MH:Pune:BLD1.

Thus, for Border-to-Border policies, the policy tree gets constructed to fit best in the existing source and target branches. Consider sharing as many nodes as possible as preferable.

Logical Partitioning Policy Search Algorithm

In Release 7.1(2) of the *Cisco Unified Communications Manager Features and Services Guide,* the "Logical Partitioning" chapter provides a list of steps that take place during a policy search. Find these steps in the Logical Partitioning Policy Search Algorithm section. The following content replaces the content in the Basic Operation subsection of Release 7.1(2) of the document, including an expanded and corrected list of steps.

Basic Operation

Construct a list of name/value pairs from the geolocation and geolocation filter information (that is, pairList1 and pairList2).

Example: pairList =”Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”

Input for the search specifies {pairList1, devType1}, {pairList2, devType2}.

The following steps take place during the policy search:

Step 1 If devType1=Border and devType2=Interior, set {devTypeA=devType1, pairListA= pairList1} and {devTypeB=devType2, pairListB= pairList2}.

Step 2 If devType1=Interior and devType2=Border, set {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.

Step 3 Match the exact pair by searching the nodes of a policy tree. Use values from {devTypeA, pairListA} and find the source branch of the tree.

Step 4 Use values from {devTypeB, pairListB} and find the target (paired) branch of the tree.

Step 5 If an exact match is found in the tree and the policy is configured, use the policy data that is configured in the leaf node and return the policy value.

Step 6 If exact match is not found, find a match by stripping one column from pairListB input (that is, go one level up on target [paired] branch of policy tree and check whether policy data is configured in the corresponding node).

Step 7 If a match is found, return the policy value; otherwise, continue going up the paired branch of the policy tree and check whether policy data is configured.

Step 8 If a policy is not found, go one level (node) up on the source branch that corresponds to pairListA.

Step 9 Repeat Step 4 through Step 8 until a policy is found or the root node is reached.

Step 10 If devType1=Border and devType2=Border, search for exact match by traversing. Use {devTypeA=devType1, pairListA= pairList1}, and {devTypeB=devType2, pairListB= pairList2}. If not found, traverse and use {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.

Note The tree layout can specify any order, based on how the administrator added policies, so you need to use both combinations to search the tree.

Redirected Dialed Number Identification Service and Diversion Header

Releases 6.1(4) and 7.1(3) add the Redirected Dialed Number Identification Service (RDNIS) and diversion header capability for certain calls that use the Cisco Unified Mobility Mobile Connect feature.

The RDNIS/diversion header for Mobile Connect enhances this Cisco Unified Mobility feature to include the RDNIS or diversion header information on the forked call to the mobile device. Service providers and customers use the RDNIS for correct billing of end users who make Cisco Unified Mobility Mobile Connect calls.

For Mobile Connect calls, the Service Providers use the RDNIS/diversion header to authorize and allow calls to originate from the enterprise, even if the caller ID does not belong to the enterprise Direct Inward Dial (DID) range.

Example Use Case

Consider a user that has the following setup:

Desk phone number specifies 89012345.

Enterprise number specifies 4089012345.

Remote destination number specifies 4088810001.

User gets a call on desk phone number (89012345) that causes the remote destination (4088810001) to ring as well.

If the user gets a call from a nonenterprise number (5101234567) on the enterprise number (4089012345), the user desk phone (89012345) rings, and the call gets extended to the remote destination (4088810001) as well.

Prior to the implementation of the RDNIS/diversion header capability, the fields populated as follows:

Calling Party Number (From header in case of SIP): 5101234567

Called Party Number (To header in case of SIP): 4088810001

After implementation of the RDNIS/diversion header capability, the Calling Party Number and Called Party Number fields populate as before, but the following additional field gets populated as specified:

Redirect Party Number (Diversion Header in case of SIP): 4089012345

Thus, the RDNIS/diversion header specifies the enterprise number that is associated with the remote destination.

Configuration in Cisco Unified Communications Manager Administration

To enable the RDNIS/diversion header capability for Mobile Connect calls, ensure the following configuration takes place in Cisco Unified Communications Manager Administration:

All gateways and trunks must specify that the **Redirecting Number IE Delivery — Outbound** check box gets checked.

In Cisco Unified Communications Manager Administration, you can find this check box by following the following menu paths:

For H.323 and MGCP gateways, execute **Device > Gateway** and find the gateway that you need to configure. In the Call Routing Information - Outbound calls pane, ensure that the **Redirecting Number IE Delivery - Outbound** check box gets checked. For T1/E1 gateways, check the **Redirecting Number IE Delivery - Outbound** check box in the PRI Protocol Type Information pane.

- For SIP trunks, execute **Device > Trunk** and find the SIP trunk that you need to configure. In the Outbound Calls pane, ensure that the **Redirecting Diversion Header Delivery - Outbound** check box gets checked.

SIP Gateway Protocol Supports Mobile Voice Access

Release 7.1(3) of Cisco Unified Communications Manager adds the SIP gateway protocol to the existing H.323 gateway protocol that supports the Mobile Voice Access feature as part of Cisco Unified Mobility capabilities.

The updates that follow apply to the documentation that displays on Cisco.com at this URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmfeat/fsmobmgr.html

Restrictions

Gateways and Ports

Only H.323 and SIP gateways get supported for Mobile Voice Access.

Configuring an H.323 or SIP Gateway for System Remote Access

If you already have an H.323 or SIP gateway that is configured in Cisco Unified Communications Manager, you can use it to support system remote access. If you do not have an H.323 or SIP gateway, you must add and configure one. For more information, refer to the "Adding a Cisco IOS H.323 Gateway" section in the *Cisco Unified Communications Manager Administration Guide*.

Note When a Mobile Connect call is placed from an internal extension, the system presents only the internal extension as the caller ID. If an H.323 or SIP gateway is used, you can use translation patterns to address this issue.

The following sample configuration for SIP gateway voip dial-peer is added at the end of Step 5 of the procedure in this section:

Sample configuration for SIP gateway voip dial-peer:

- dial-peer voice 80 voip
- destination-pattern <Mobile Voice Access DN>
- rtp payload-type nse 99
- session protocol sipv2
- session target ipv4:10.194.107.80
- incoming called-number .T
- dtmf-relay rtp-nte
- codec g711ulaw

Support for Microsoft Active Directory Application Mode LDAP Server

Cisco Unified Communications Manager can synchronize with Microsoft Active Directory Application Mode LDAP server, in addition to the previously supported LDAP servers. This release supports the following LDAP servers:

- Microsoft Active Directory 2000
- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- Microsoft Active Directory Application Mode 2003
- Microsoft Active Directory Application Mode 2008 (AD LDS)
- iPlanet Directory Server 5.1
- Sun ONE Directory Server 5.2
- Sun ONE Directory Server 6.x
- OpenLDAP 2.3.39
- OpenLDAP 2.4

Be aware that Microsoft Active Directory Application Mode support is limited to those directory topologies that are already supported with a native Active Directory connection. No additional topologies, such as multiforest, multitree single forest, or global catalog get supported.

Follow these steps to synchronize with a Microsoft Active Directory Application Mode LDAP server:

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration.

Step 2 Choose **System > LDAP > LDAP System**.

Step 3 Check the **Enable Synchronizing from LDAP Server** check box.

Step 4 From the LDAP Server Type list, choose **Microsoft Active Directory Application Mode**.

Step 5 From the LDAP Attribute for User ID list, choose an LDAP attribute value for the user ID.

Step 6 Click the **Save** button.

Step 7 Choose **System > LDAP > LDAP Directory**.

Step 8 Click the **Add New** button.

Step 9 Enter the appropriate settings as described in Table 1-3.

Step 10 Click the **Save** button.

Table 1-3 LDAP Directory Configuration Settings

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Reenter the password that you provided in the LDAP Password field.
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.
LDAP Directory Synchronization Schedule	
Perform Sync Just Once	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database only once, check this check box.
Perform a Re-sync Every	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database at a regular interval, use these fields. In the left field, enter a number. In the drop-down list box, choose a value: • hours • days • weeks • months Cisco Unified Communications Manager can synchronize directory information every 6 hours, which is the minimum value that is allowed for this field. **Note** This field remains active only if you do not check the Perform Sync Just Once check box.
Next Re-sync Time (YYYY-MM-DD hh:mm)	Specify a time to perform the next synchronization of Cisco Unified Communications Manager directory data with this LDAP directory. Use a 24-hour clock to specify the time of day. For example, 1:00 pm equals 13:00.

Table 1-3 LDAP Directory Configuration Settings (continued)

Field		Description
User Fields To Be Synchronized		
Cisco Unified Communications Manager User Fields	**LDAP User Fields**	
User ID	One of the following: uid userprincipalName mail employeeNumber telephoneNumber	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right.
Middle Name	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • middleName • initials
Manager ID	manager	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right.
Phone Number	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • telephoneNumber • ipPhone
First Name	givenName	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right.
Last Name	sn	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right.
Department	department number	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right.

Table 1-3 LDAP Directory Configuration Settings (continued)

Field		Description
Mail ID	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field that is specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • mail • uid
LDAP Server Information		
Host Name or IP Address for Server		Enter the host name or IP address of the server where the data for this LDAP directory resides.
LDAP Port		Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. 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: **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.) **Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

Table 1-3 LDAP Directory Configuration Settings (continued)

Field	Description
Use SSL	Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes. **Note** If LDAP over SSL is required, ensure the corporate directory SSL certificate is loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* documents the certificate upload procedure in the "Security" chapter.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server.

In addition to the user fields that display in Cisco Unified Communications Manager Administration, the user fields that are described in Table 4 also get synchronized.

Table 4 Additional Synchronized User Fields

Cisco Unified Communications Manager User Fields	LDAP User Fields
UniqueIdentifier	ObjectGUID
Pager	pager or pagertelephonenumber
Mobile	mobile or mobiletelephonenumber
Title	title
Homephone	homephone or hometelephonenumber
OCSPrimaryUserAddress	msRTCSIP-primaryuseraddress

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(3), 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:

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 49.

Cisco Unified IP Phones

Beginning with Cisco Unified Communications Manager Release 7.1(3), 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(3), 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

The following devices support a trusted connection:

- Cisco Unified IP Phone 7960G/7940G
- Cisco Unified IP Phone 7906G/7911G
- Cisco Unified IP Phone 7931G

- Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G/7971G-GE
- Cisco Unified IP Phone 7975G
- Cisco Unified Wireless IP Phone 7921
- Cisco Unified Wireless IP Phone 7925
- Cisco IP Communicator, CSF model
- Cisco TelePresence Phones:

  Cisco TelePresence System 500

  Cisco TelePresence System 1000

  Cisco TelePresence System 3000

  Cisco TelePresence System 3200

Bulk Administration Tool

This section contains information on the following topics:

- Support for Feature Control Policy, page 50
- BAT Support for New Limits for Speed Dials, BLF Speed Dials, and BLF Directed Call Park, page 50
- Inserting User Device Profiles and Phones into Cisco Unified Communications Manager, page 51

Support for Feature Control Policy

Feature Control Policy requires additional phone support to work. At this time, if you configure feature control policy, the functionality does not work.

BAT Support for New Limits for Speed Dials, BLF Speed Dials, and BLF Directed Call Park

BAT now supports a maximum of 199 Speed Dials, 199 BLF Speed Dials, and 199 BLF Directed Call Park instances. The Bulk Administration GUI includes the following updates to support this change:

- Phone Template, UDP Template, Phone - Create File Format and UDP - Create File Format pages support the new limit for Speed Dials, BLF Speed Dials, and BLF Directed Call Park.
- Insert, Export, and Validate Details—The following insert, export, and validate details features have support for the new limit for Speed Dials, BLF Speed Dials, and BLF Directed Call Park:

  Insert Phones Specific Details

  Insert Phones All Details

  Export Phones Specific Details

  Export Phones All Details

Validate Phones All Details

Validate Phones Specific Details

Insert Phones/Users

Validate Phones/Users

Insert UDP All Details

Insert UDP Specific Details

Export UDP All Details

Export UDP Specific Details

Validate UDP All Details

Validate UDP Specific Details

- BAT xlt Support for the New Limit for Speed Dials, BLF Speed Dials, and BLF Directed Call Park—BAT.xlt provides support for the new limit for Speed Dials, BLF Speed Dials, and BLF Directed Call Park in the Phones, UDP, and Phones and Users sheets. You can use the BAT.xlt to add or update the Speed Dials, BLF Speed Dials, and BLF Directed Call Park details.

Note Be aware that the maximum number of columns that can be configured by using bat.xlt is limited due to the Microsoft Excel limitation of 256 columns.

Inserting User Device Profiles and Phones into Cisco Unified Communications Manager

While you are inserting user device profiles for user devices and inserting phones into Cisco Unified Communications Manager, the following check boxes get enabled for selection after you have checked the **Override the existing configuration** check box.

- Delete all existing speed dials before adding new speed dials.
- Delete all existing BLF Speed Dials before adding new BLF Speed Dials.
- Delete all existing Subscribed Services before adding new services.

Note Check the check box(es) to delete all existing Speed Dials, BLF Speed Dials, or Subscribed Services records and add new records. Leave the check box(es) unchecked if you want to append these to existing records.

Cisco Unified IP Phones

This section provides the following information:

- Cisco Unified IP Phone 6900 Series, page 52
- Secure SIP Failover for SRST, page 53
- Feature Key Capacity Increase for Cisco Unified IP Phones, page 54
- SIP Digest Authentication Name, page 55

Cisco Unified IP Phone 6900 Series

The Cisco Unified IP Phone 6900 Series, a new and innovative portfolio of endpoints, delivers affordable, business-grade, voice communication services to customers worldwide. Three models are available:

- Cisco Unified IP Phone 6921 (two-line)
- Cisco Unified IP Phone 6941 (four-line)
- Cisco Unified IP Phone 6961 (twelve-line)

All three models support the following features:

- two colors and two hand set style options
- full-duplex speakerphones
- single-call per-line appearance
- buttons for hold, transfer, and conference
- buttons for Directory, Settings, and Messages
- four softkey buttons and a scroll toggle bar
- tricolor LED line and feature keys
- right-to-left language presentation on the displays
- network features that include Cisco Discovery Protocol and IEEE 802.1 p/q tagging and switching
- 10/100BASE-T Ethernet connection through two RJ-45 ports, one for the LAN connection and the other for connecting a downstream Ethernet device such as a PC
- G.711a, G.711, G.729a, G.729b, and G.729ab audio-compression codecs
- power from IEEE 802.3af-compliant blades
- use of reground and recyclable plastics
- the following American Disabilities Act (ADA) features:

  The hearing-aid-compatible (HAC) hand set meets the requirements that the ADA sets.

  HAC meets ADA HAC requirements for a magnetic coupling to approved hearing aids.

  The phone dialing pad complies with ADA standards.

For more information, click the following URL:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10326/data_sheet_c78-541199.html

Requirements

The Cisco Unified IP Phone 6900 Series requires the following release:

- Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition Versions 7.1.2 and later that are using Skinny Client Control Protocol (SCCP).

Where to Find More Information

- *Cisco Unified IP Phone 6921, 6941, and 6961 User Guide for Cisco Unified Communications Manager 7.1 (SCCP)*
- *Cisco Unified IP Phone 6921, 6941, and 6961 Administration Guide for Cisco Unified Communications Manager 7.1 (SCCP)*

- *Cisco Unified IP Phone 6961 for Administrative Assistants Quick Start*
- *Cisco Unified IP Phone 6921 Quick Start*

Secure SIP Failover for SRST

Firmware release 8.5(3) provides support for secure calls on a Cisco Unified IP Phone that is running SIP to remain secure after the call fails over to SRST from Cisco Unified Communications Manager. In addition, this feature allows the user to verify that the call is still secure by the lock icon that remains on the phone display.

The SRST supports RTP and SRTP media connections according to how the security settings are configured on the IP phone.

The system administrator configures SRST on a Cisco router to allow endpoints that are using SIP to register to SRST by using SIP/UDP, SIP/TCP, and SIP/TLS/TCP.

The following example shows a complete secure configuration for the SRST:

```
voice service voip
srtp fallback
allow-connections sip to h323
allow-connections sip to sip
sip
    url sips
    srtp negotiate cisco
voice register global
security-policy secure
sip-ua
registrar ipv4:101.2.0.10 expires 3600
xfer target dial-peer
crypto signaling default trustpoint 3745-SRST strict-cipher
```

Note The default value for the CLI command security-policy specifies **device-default**. If the value is set to the default value, the existing transport mechanism will get accepted by and registered to the SRST on failover. If the value is set to **secure**, the SRST will only accept the following transport mechanisms to ensure that the call maintains its secure state, if applicable—SIP/TLS/TCP.

The following example shows a complete device-default configuration for the SRST:

```
voice service voip
srtp fallback
allow-connections sip to h323
allow-connections sip to sip
sip
    url sip
    srtp negotiate cisco
voice register global
default security-policy
sip-ua
registrar ipv4:101.2.0.10 expires 3600
xfer target dial-peer
crypto signaling default trustpoint 3745-SRST
```

Beginning in firmware release 8.5(3), when an IP phone endpoint that is using SIP is in a secure call that fails over to SRST from Unified CM, the user will continue to see the lock icon on the phone display, which indicates that the call remains secure. In previous releases, a SIP/TLS/TCP call that fails over to SRST displays the play arrow icon to indicate a non-secure call.

When IP phones register to the SRST, if all segments of the call are SIP endpoints, all the supplementary features get supported—conference, transfer, blind transfer, and call forward. If the segments of the call are both SIP and SCCP endpoints, only basic call gets supported.

This feature gets supported on the following IP phones:

- 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 7911G
- Cisco Unified IP Phone 7906G

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*
- *PI12 ARTG BU Special Release Notes*

Feature Key Capacity Increase for Cisco Unified IP Phones

The feature key capacity increase for Cisco Unified IP Phones allows administrators to use all 48 additional keys on Cisco Unified IP Phone Expansion Modules 7915 and 7916.

You can configure a maximum of 56 keys for a Cisco Unified IP Phone 7975G, and you can configure up to 54 keys for Cisco Unified IP Phones 7965G and 7962G.

The line capability increase includes Directory Numbers (DN), line information menu, line ring menu, and line help ID.

Table 5 Phone Models and Maximum Directory Numbers Configurable

Phone Model	Programmable Buttons	Maximum Directory Numbers
Cisco Unified IP Phone 7962G	6	54
Cisco Unified IP Phone 7965G	6	54
Cisco Unified IP Phone 7975G	8	56

Note Cisco Unified IP Phone 7975G includes eight programmable buttons; therefore, it supports 56 DNs. Cisco Unified IP Phones 7965G and 7962G have six programmable buttons; therefore, the maximum number of DNs that are available for these phones equals 54.

This feature gets supported on the following IP phones (SCCP and SIP):

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*

SIP Digest Authentication Name

The length of the SIP digest authentication name increased to 128 characters for Cisco Unified IP Phones (SIP):

The authentication name only gets used if the Enable Digest Authentication check box is checked in the Phone Security Profile Configuration window. The authentication name derives from the User ID of the end user who is assigned to the phone.

This feature gets supported on the following IP phones (SIP):

- 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 7911G
- Cisco Unified IP Phone 7906G

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*

Table 6 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.1(3) Features

Cisco Unified Communications Manager 7.1(3) Feature	Cisco Unified IP Phone Support	For more information, see
Cisco Unified IP Phone 6900 Series	SCCP only 6921 6941 6961	Cisco Unified IP Phone 6900 Series, page 52
Secure SIP Failover for SRST	SIP: 7906G 7911G 7931G 7941G 7941G-GE 7961G 7961G-GE 7942G 7962G 7945G 7965G 7970G 7971G 7975G	Secure SIP Failover for SRST, page 53
Feature Key Capacity Increase for Cisco Unified IP Phones	SCCP and SIP: 7962G 7965G 7975G	Feature Key Capacity Increase for Cisco Unified IP Phones, page 54 DN Capacity Increase for the Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 38
SIP Digest Authentication Name	SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G	SIP Digest Authentication Name, page 55

Cisco Unified Serviceability and RTMT

This section contains information on the following topics:

- Feature Control Policy Support in RTMT and Cisco Unified Serviceability, page 57

Feature Control Policy Support in RTMT and Cisco Unified Serviceability

Performance monitor counters display in RTMT for feature control policy. Because feature control policy relies on additional phone support, which is not available at this time, the performance monitoring counters do not work.

Updated TFTP alarms exist in Cisco Unified Serviceability to support feature control policy. Because feature control policy relies on additional phone support, which is not available at this time, the alarms do not get generated for the feature.

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.

UsingBug 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(3) As of September 14, 2009 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(3) As of September 14, 2009" section on page 59 to access the online record for that defect, including workarounds.

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

When you open the online record for a defect, you will see data in the "First Fixed-in Version" field. The information that displays in this field identifies the list of 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(3) As of September 14, 2009" section on page 59 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "UsingBug Toolkit" section on page 57.

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(3) As of September 14, 2009

The following information comprises unexpected behavior (as of September 14, 2009) that you may encounter in Release 7.1(3) of Cisco Unified Communications Manager.

Table 7 Open Caveats as of September 14, 2009

CSCtb78875	axl	VG224 query with empty lines parameters does not remove line associations.
CSCta95472	axl	AXL service stuck contacting offline subscribers.
CSCtb72879	axl	User AXL API does not have tags to update CTI controlled device profiles.
CSCtb79428	axl	Some getDeviceProfile requests fail with error.
CSCtb01481	backup-restore	DRS page does not time out after remaining idle for 30 minutes.
CSCta18902	cli	Upgrade process does not exit after error.
CSCtb75135	cli	When a CLI based upgrade cannot start due to a lock error (e.g. - a DRS backup/restore has locked the server), the CLI command appears to freeze instead of displaying the correct lock message.
CSCta97266	cmcti	CTIManager cores when run traffic with L2 upgrade and memory leaking.
CSCtb49103 STAYS	cmcti	CTI reports incorrect partition information.
CSCsx68761 STAYS	cmcti	Duplicate callPartyInfoChangedEvent when drop party across cluster.
CSCsr30432 STAYS	cmcti	Unified CM does not send NOTIFY.
CSCsz28237 STAYS	cm-docs	Call Park displays invalid park number.
CSCtb89595	cmui	CUMA security profile add is inconsistent. It allows copy.

CSCtb89807	cmui	User cannot change owner user ID on EM-enabled phone when logged out.
CSCtb34945	cmui	Missing Find and List in title of Find and List windows
CSCtb75150	cmui	When a DRS lock exists or DRS is running, COP file install problems exists.
CSCta44791	cmui	HTTP 404 error on Cisco Unified CM admin help.
CSCtb51861 STAYS	cp-mediacontrol	7985 No video exists on H323 ICT between Unified CM 4.2 and 7.1.
CSCtb58536	cp-mediacontrol	DTMF does not work after agent drops.
CSCtb57437 STAYS	cp-mediacontrol	Unified CM media layer does not handle the 488 response from peer.
CSCsy62649 STAYS	cp-mediacontrol	Call drops after a sequence of blind and supervised transfers.
CSCtb08088	cp-sccp	The shield icon is missing if an auth IPv6 phone calls an auth IPv4 telephone.
CSCta39095 STAYS	cp-sccp	Unified CM does not allow SCCP phone to drop basic and whisper calls together.
CSCtb59075	cp-sip-station	SIPStationInit rejects calls with 503 cause code, so BB calls fail.
CSCtb73697	cp-sip-trunk	DSCP signaling packets set to Best Effort on outgoing SIP calls.
CSCtb13814 STAYS	cp-sip-trunk	When the SDP offer contains X-NSE&G729, Unified CM sets SDP answer with G729Annexb.
CSCtb89537	cp-system	Alarm definition SDLLinkOOS of Unified CM contains CTIManager.
CSCtb66354	cpi-os	IBM Director Agent reports defunct drive - false RAID alert.
CSCtb01996 STAYS	cpi-os	DNS query gets sent using IPv6 even though IPV6 is not enabled on Unified CM.
CSCsz34001 STAYS	cpi-os	HIgh CPU and IOwait occurs during load.
CSCtb50449	cpi-os	IBM 7835/45-I3 servers need critical raid firmware update.
CSCtb83367	cpi-os	/usr/bin/script generates core.
CSCsl81015 STAYS	cpi-security	Critical sshd[32211]: fatal: Write failed: Connection reset by peer.
CSCta20132 STAYS	cuc-tomcat	Continuous webapps start/stop causes low permgen memory.
CSCtb08166	database	SIP phone does not follow the setting of Off-hook to First Digit timer.
CSCtb77511	database-ids	Need exists for code changes.
CSCtb67775	qed	Unified CM does not make proper configuration for MGCP gateway on WIC.

CSCsv95745 STAYS	rtmt	RTMT: the create directory button appears disabled.
CSCtb61583 STAYS	serv-soap	AXL LogCollectionPort SelectLogFiles ZipInfo does not compress files.
CSCta45016 STAYS	syslog	Alarms do not get sent to remote syslog whenthey get configured under serviceability.
CSCtb86269	tapisdk	TSP stopped working after upgrade to Unified CM 7.13 version of TSP.
CSCtb78022	tapisdk	TFTP IPAddress value is not updated in registry for Windows Vista.
CSCtb80964	tapisdk	Race condition caused by remote access connection does not get handled properly.
CSCtb52560	voice-sipstack	Cisco Unified CM sends ACK/BYE at timer expiry.

Documentation Updates

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

- Installation, Upgrade, and Migration, page 61
- Server Replacement, page 63
- Troubleshooting, page 63
- Bulk Administration Tool, page 64
- Cisco Unified Communication Manager CDR Analysis and Reporting, page 65
- Cisco Unified Communications Manager Security, page 66
- Cisco Unified Communications Operating System, page 67
- Cisco Unified Communications Manager Administration, page 69
- Cisco Unified Serviceability, page 82

Installation, Upgrade, and Migration

This section contains information on the following topics:

- Installation, Upgrade, and Migration, page 61

Installing Licenses While Replacing a Publisher Node

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

Table 8 Replacing the Publisher Node Process Overview

	Description	For More Information
Step 1	Perform the tasks in the "Server or Cluster Replacement Preparation Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*
Step 2	Gather the necessary information about the old publisher server.	See the "Gathering System Configuration Information to Replace or Reinstall a Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 3	Back up the publisher server to a remote SFTP server by using the Disaster Recovery System and verify that you have a good backup.	See the "Creating a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 4	Get new licenses of all the license types before system replacement.	Get new licenses of all the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. You only need new licenses if you are replacing the publisher node. For more information, see the "Obtaining a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 5	Shut down and turn off the old server.	
Step 6	Connect the new server.	
Step 7	Install the same Cisco Unified Communications Manager release on the new server that was installed on the old server, including any Engineering Special releases. Configure the server as the publisher server for the cluster.	See the "Installing Cisco Unified Communications Manager on the New Publisher Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 8	Restore backed-up data to the publisher server by using Disaster Recovery System.	For more information, see the "Restoring a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 9	Reboot all nodes in the cluster. If the server is not in a cluster, then reboot the server.	
Step 10	Upload all of the new license files to the publisher server.	Upload new license files for all of the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. For more information, see the "Uploading a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 11	Delete all invalid license files (those based on the old server MAC address).	"Deleting Invalid License Files" section on page 63
Step 12	Perform the post-replacement tasks in the "Post-Replacement Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*

Deleting Invalid License Files

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

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

The MAC address displays in the field License MAC.

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

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

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

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

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

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

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

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

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

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

Server Replacement

This section contains information on the following topics:

- Password Validation During a Server Replacement, page 63

Password Validation During a Server Replacement

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

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

Troubleshooting

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

Two New dbreplication Commands Exist

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

utils dbreplication runtimestate

Use this command

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

utils dbreplication quickaudit

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

Bulk Administration Tool

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

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

Deleting Unassigned Directory Numbers

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

Procedure

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

The Delete Unassigned Directory Numbers window displays.

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

- Pattern
- Description
- Route Partition

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

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

Step 3 Specify the appropriate search text, if applicable.

Step 4 Click **Find**.

A list of discovered phones displays by

- Pattern
- Description
- Partition

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

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

The default description is Delete Unassigned DN - Query

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

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

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

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

Cisco Unified Communication Manager CDR Analysis and Reporting

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

- Changed Values of Mobility Cell Pick, page 65
- Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting, page 66
- "Mailing a Report" Recipients, page 66

Changed Values of Mobility Cell Pick

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

FieldNames	Enterprise Call to 22285	Server Call to Cell Phone	Final Handout Call
callingPartyNumber	22202	2202	22202
originalCalledPartyNumber	22285	22285	22285
finalCalledPartyNumber	22285	9728324124	22285
lastRedirectDn	22285	22285	22285
origCause_Value	393216	393216	0
dest_CauseValue	393216	393216	16
lastRedirectRedirectReason	0	0	415

lastRedirectRedirectOnBehalfOf	0	24	24
joinOnBehalfOf	0	24	24

Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting

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

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

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

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

"Mailing a Report" Recipients

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

When the Mailing option gets enabled,

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

Cisco Unified Communications Manager Security

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

You Can Use HTTPS Protocol with Different Browsers and Operating Systems

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

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

Definition of Locally Significant Certificate

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

Cisco Unified Communications Operating System

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

Incorrect Values for Phase One DH an dPhase Two DH

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

Using Certificates Issued by a Third-Party Certificate Authority

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

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

  The CAPF CSR uses the following extensions:

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

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

  ```
  X509v3 Key Usage:
  Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
  ```

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
```

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

Revised Procedure to Shut Down the System

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

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

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

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

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

- Replace the note text with the following text:

  The hardware may require several minutes to power down.

- Insert the following text after the note:

  Procedure 2

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

Disk Space Before Upgrading

Before you upgrade to Cisco Unified Communications Manager from supported appliance releases, make sure that you have enough disk space on the common partition to perform the upgrade. To ensure that you have enough disk space, determine the size of the ISO file on your DVD or on Cisco.com. If you are upgrading from a local source (DVD), you need the same amount of disk space as the size of the ISO file. If you are upgrading from a network source, you need twice the amount of disk space as the size of the combined ISO file.

To verify the disk space on the common partition, do one of the following tasks:

- Use the **show status** CLI command and note the information that displays under the Disk/logging heading.
- From Cisco Unified Communications Operating System, choose **Show > System**.

- From Cisco Unified Real-Time Monitoring Tool, choose **System > Server > Disk Usage**. Choose the server from the Disk Usage at Host drop-down list box and view the Used Space (MB) for the Common partition.

If you do not have enough disk space, use Cisco Unified Real-Time Monitoring Tool to collect core and trace files and delete them from the server. For more information on collecting files, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

You can also use the log partition monitoring service or the command line interface (CLI) to delete files on your server; however, Cisco does not recommend using these tools to delete files during regular business hours, as they can impact system performance. For more information on configuring log partition monitoring, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For more information on the CLI, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 7.1(3)*.

Note To prevent disk usage issues due to large numbers of trace files in the future, you should review your trace configuration settings in Cisco Unified Serviceability (**Trace > Configuration**). You can reduce the maximum number of trace files for your services or set the trace settings to the default values.

Pre-Upgrade Task Is Omitted From Software Upgrades Chapter

The “Software Upgrades” chapter in the *Cisco Unified Communications Operating System Administration Guide* omits the following pre-upgrade task:

Before you perform the Cisco Unified Communications Manager 7.1(3) upgrade, ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.

Cisco Unified Communications Manager Administration

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

Cisco Unified Communications Manager Administration Guide

- How the Number of Client Matter Codes Affects System Start Up Time, page 71
- SIP Profile Configuration No Longer Includes a Call Stats Check Box, page 71
- NTP Reference Configuration Settings Omits Two Available Modes, page 71
- IP Subnet Example Incorrectly Contains a Period (.) Instead of a Slash (/), page 71
- Default Setting of the User Must Change at Next Login Check Box Is Incorrect, page 72
- Device Name Field Omits Information About Valid Characters and Number of Characters Allowed, page 72
- Valid Characters Not Included in the Description of the Transcoder Device Name Field, page 72
- Valid Characters Not Included in the Description of the IOS Conference Bridge Name Field, page 72
- Invalid Characters for Cisco Conference Bridge (WS-SVC-CMM) Description Field Omitted, page 72
- Application Dial Rule Configuration Settings Table Is Incorrect, page 73

Cisco Unified Communications Manager System Guide

Cisco Unified Communications Manager Features and Services Guide

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

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

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

SIP Profile Configuration No Longer Includes a Call Stats Check Box

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

That check box no longer exists.

NTP Reference Configuration Settings Omits Two Available Modes

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

The additional information specifies:

- Multicast
- Anycast

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

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

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

The examples should specify:

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

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

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

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

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

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

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

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

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

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

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

That information follows:

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

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

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

That information follows:

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

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

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

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

Application Dial Rule Configuration Settings Table Is Incorrect

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

Table 9 Application Dial Rule Configuration Settings

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

Valid Characters for Voice Mail Profile Name Field Omitted

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

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

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

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

User Documentation Misnames Single Button Barge Field

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

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

Allowed Prefix Digits Incorrect for AAR Group Configuration

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

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

Service Parameters Expanded Explanation

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

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

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

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

Note

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

Number of Locations and Regions That Cisco Unified Communications Manager Supports

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

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

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

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

Intercom Route Partition Configuration Settings Description Field Information Is Incorrect

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

Valid Characters in Name Field of Role Configuration Window

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

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

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

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

Incorrect Information

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

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

- Forwards the name of the caller that is assigned to the directory number.
- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration.

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

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

Correct Information

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

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

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

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

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

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

End User Chapter Includes Incorrect Information for Manager User ID Field

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

Incorrect Description

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

Correct Description

For the Manager User ID field, enter the user ID of the end user manager ID..

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recording Destination Address Field Description

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

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

Call Stats Check Box Not Available to Enable Voice Quality Metrics

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

That check box no longer exists.

Number of Digits Field Description Is Incorrect

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

The correct information follows:

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

OpenLDAP Version 2.3.41 Not Listed in LDAP Synchronization Documentation

The "Understanding the Directory" chapter in the *Cisco Unified Communications Manager System Guide* does not state the version of OpenLDAP that is supported for LDAP Synchronization with Cisco Unified Communications Manager Release 7.1(3). To identify the supported version, see the OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database, page 32.

Application Dial Rules Configuration Error Checking Information Is Incorrect

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

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

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

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

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

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

Example

Consider the following example:

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

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

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

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

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

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

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

Barge Initiators Cannot Conference In Additional Callers

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

- The barge initiator cannot conference in additional callers.

IPMASecureSysUser Password Change Procedure

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

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

CSCsy92863 Intercom Route Partition Online Help Is Incorrect

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

Mobile Connect Support Restrictions

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

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

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

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

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

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

Enterprise Feature Access Two-Stage Dialing

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

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

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

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

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

Valid Characters in Name Field of Access List Configuration Window

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

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

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

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

Name

> Enter a text name for the remote destination profile.
>
> This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Description

> Enter a text description of the remote destination profile.
>
> This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Filter Configuration Window

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

> Enter a unique name for this geolocation filter. Default name cannot be blank.
>
> This field can contain up to 50 ASCII characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Configuration Window

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

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

Intercom Calls Cannot Be Placed on Hold

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

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

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

The following document omits this limitation:

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

Mobile Voice Access Directory Number Field Description

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

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

Cisco Unified Serviceability

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

- Password Description Omitted, page 83

Password Description Omitted

The Application Billing Server Parameter Settings table in “Configuring CDR Repository Manager” chapter of the Cisco Unified Communications Manager Serviceability Guide omits this information:

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

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.