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

Updated January 21, 2013

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

Caution Because Cisco Unified CM 7.1(3) does not contain many of the fixes included in Cisco Unified CM 6.1(5), do not upgrade from Unified CM 6.1(5) to Unified CM 7.1(3x).

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

Cisco Unified Communications Manager Release 7.1(3b) resolves one defect. See CSCtc80749 Server Boot Up Time Increases With Each Reboot and Hardware SNMP Fails, page 17. There are no new features.

- Introduction, page 2
- System Requirements, page 2
- Upgrading to Cisco Unified Communications Manager 7.1(3b), page 4
- Service Updates, page 13
- Related Documentation, page 13
- Important Notes, page 14
- New and Changed Information, page 38
- Caveats, page 76
- Documentation Updates, page 80
- Obtaining Documentation and Submitting a Service Request, page 80

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.

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

Before you install or upgrade Cisco Unified Communications Manager, Cisco recommends that you review the "Upgrading to Cisco Unified Communications Manager 7.1(3b)" section on page 4, and the "Service Updates" section on page 13 for information pertinent to installing or upgrading, and the "Important Notes" section on page 14 for information about issues that may affect your system.

Note To ensure continuous operation and optimal performance of your Cisco Unified Communications Manager system, you should upgrade to Cisco Unified Communications Manager 7.1(3x).

Introduction

Cisco Unified Communications Manager, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

System Requirements

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

- Supported Cisco Unified Communications Manager Releases by Server, page 2
- Cisco Unified Communications Manager Software Compatibility Matrix, page 2
- Uninterruptible Power Supply, page 3

Supported Cisco Unified Communications Manager Releases by Server

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 Supported Cisco Unified Communications Manager Releases by Server: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.

Cisco Unified Communications Manager Software Compatibility Matrix

Be aware that some servers that are listed in the *Cisco Unified Communications Manager Software Compatibility Matrix* (http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html) may require additional hardware support for Cisco Unified CM Release 7.1(3b). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the *Cisco Unified Communications Manager Software Compatibility Matrix*. Cisco Unified CM requires a minimum of 2 GB of memory, 72 GB disk drive, and 2 GHz processor.

Uninterruptible Power Supply

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

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

When Cisco Unified Communications Manager runs on one of the servers that are listed in Table 1, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported.

Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported with the APC SmartUPS 1500VA USB and APC 750VA XL USB. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, you can execute the CLI command **show ups status** that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started. The CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime, and other relevant status information.

When the feature is activated, graceful shutdown will commence as soon as the low battery threshold is reached. Resumption or fluctuation of power will not interrupt or abort the shutdown, and administrators cannot stop the shutdown after the feature is activated.

For unsupported Cisco Unified Communications Manager releases, MCS models and/or UPS vendor/make/models, you can cause an external script to monitor the UPS. When low battery gets detected, you can log on to Cisco Unified Communications Manager by using Secure Shell (SSH), access the CLI, and execute the **utils system shutdown** command.

Table 1 Supported Servers for Basic Integration

HP Servers	IBM Servers
MCS-7816-H3	MCS-7815-I1
MCS-7825-H1	MCS-7815-I2
MCS-7825-H2	MCS-7816-I3
MCS-7825-H3	MCS-7816-I3
MCS-7825-H4	MCS-7825-I1
MCS-7828-H3	MCS-7825-I2
MCS-7828-H4	MCS-7825-I3
MCS-7835-H2	MCS-7825I-30
MCS-7845-H2	MCS-7825-I4
MCS-7835-H3	MCS-7828-I3
MCS-7845-H3	MCS-7828-I4
	MCS-7828-I4
	MCS-7835-I1

Table 1 Supported Servers for Basic Integration

HP Servers	IBM Servers
	MCS-7835I-30
	MCS-7845-I2
	MCS-7835-I3
	MCS-7845-I3

Upgrading to Cisco Unified Communications Manager 7.1(3b)

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

- Before You Begin, page 4
- Special Upgrade Information, page 4
- Upgrade Paths to Cisco Unified Communications Manager 7.1(3b), page 8
- Ordering the Upgrade Media, page 8
- The Latest Software Upgrades for Unified CM 7.1 on Cisco.com, page 13
- Upgrading from Cisco Unified Communications Manager Release 5.1(3e) to 7.1(x) Releases, page 9
- Upgrading to Unified CM 7.1(3b) by Using the UCSInstall File, page 9
- Upgrading to Unified CM 7.1(3b) 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 4.

Note After you perform a switch version when you upgrade Unified CM, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Special Upgrade Information

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

- I/O Throttling, page 5
- Write-Cache, page 5

- Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(3x) Upgrade, page 7
- Making Configuration Changes After an Upgrade, page 7

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.

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

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

------------------------------------------------------------------------
Controller information
------------------------------------------------------------------------
   Controller Status                    : Okay
   Channel description                  : SAS/SATA
   Controller Model                     : IBM ServeRAID 8k
   Controller Serial Number             : 20ee0001
   Physical Slot                        : 0
   Copyback                             : Disabled
   Data scrubbing                       : Enabled
   Defunct disk drive count             : 0
   Logical drives/Offline/Critical      : 2/0/0
   ------------------------------------------------
   Controller Version Information
   ------------------------------------------------
   BIOS                                 : 5.2-0 (15421)
   Firmware                             : 5.2-0 (15421)
   Driver                               : 1.1-5 (2412)
   Boot Flash                           : 5.1-0 (15421)
   ------------------------------------------------
   Controller Battery Information
   ------------------------------------------------
   Status                               : Okay
   Over temperature                     : No
   Capacity remaining                   : 100 percent
   Time remaining (at current draw)     : 4 days, 18 hours, 40 minutes
   ------------------------------------------------
   Controller Vital Product Data
   ------------------------------------------------
   VPD Assigned#                        : 25R8075
   EC Version#                          : J85096
   Controller FRU#                      : 25R8076
   Battery FRU#                         : 25R8088

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

```
Write-cache setting                 : Enabled (write-back) when protected by battery
Number of chunks                    : 2
Drive(s) (Channel,Device)           : 0,2 0,3
```

Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(3x) Upgrade

Before you upgrade to Cisco Unified Communications Manager 7.1(3x), 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(3x) and the following error message gets written to the upgrade log:

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

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

Making Configuration Changes 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(3b)

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(3x), 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 *Cisco Unified Communications Manager Software Compatibility Matrix* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html) to Cisco Unified CM 7.1(3x) by using a DVD, in the Software Installation/Upgrade window, ignore the checksum step that tells you "To ensure the integrty of the installation file, verify the MD5 hash value against the Cisco Systems website." Click **Next**.

Upgrading to Unified CM 7.1(3b) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_7.1.3.30000-1.sgn.iso, comprises two parts:

- UCSInstall_UCOS_7.1.3.30000-1.sgn.iso_part1of2
- UCSInstall_UCOS_7.1.3.30000-1.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_7.1.3.30000-1 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_7.1.3.30000-1.sgn.iso_part1of2 UCSInstall_UCOS_7.1.3.30000-1.sgn.iso_part2of2 > UCSInstall_UCOS_7.1.3.30000-1.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_7.1.3.30000-1.sgn.iso_part1of2+UCSInstall_UCOS_7.1.3.30000-1.sgn.iso_part2of2 UCSInstall_UCOS_7.1.3.30000-1.sgn.iso
```

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

6180c0b0c9ff1b0893a88988c154d94b UCSInstall_UCOS_7.1.3.30000-1.sgn.iso

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

Upgrading from a Local Source

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

Procedure

Step 1 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Note Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks.

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

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

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

The Software Installation/Upgrade window displays.

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

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

Step 7 To disable throttling, check the **Disable I/O throttling** check box.

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

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

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

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

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

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

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

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

b. Click **Next**.

The Upgrade Status window displays the Upgrade log.

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

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

The system restarts running the upgraded software.

Upgrading from a Remote Source

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

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

Procedure

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

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

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

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

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

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

The Software Installation/Upgrade window displays.

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

Step 5 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

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

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

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

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

Step 10 To disable throttling, check the **Disable I/O throttling** check box.

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

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

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

Step 12 Choose the upgrade version that you want to install and click **Next**.

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

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

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

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

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

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

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

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

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

b. Click **Next**.

The Upgrade Status window displays the Upgrade log.

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

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

The system restarts and is running the upgraded software.

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.

Service Updates

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

To check for updates, from www.Cisco.com, select **Support > Download Software** . Navigate to the "Voice and Unified Communications" section and select **IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager) >** *the appropriate version of Cisco Communications Manager for your deployment*.

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

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

Related Documentation

The view documentation that supports Cisco Unified CM Release 7.1(3b), 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(3b). 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(3b).

- New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651), page 15
- Limitations to Call Park Feature, page 15
- Verify IPv6 Networking on Servers Before Upgrade, page 17
- Node Licenses Missing After an Upgrade, page 17
- CSCte56322 Netscape Browser is not Supported, page 17
- Unified CM 7.x IOS Device Does Not Offer Full NAT Support for SCCP Version 17, page 17
- CSCtc80749 Server Boot Up Time Increases With Each Reboot and Hardware SNMP Fails, page 17
- CSCtc99413 Upgrade to Unified CM 7.1(3x) from Unified CM 5.x Results in Low Active Partition Disk Alerts, page 18
- Disaster Recovery System Caution, page 18
- HP SCSI Hard Drive Firmware Update, page 18
- CSCtb95488 Phones That Support Monitoring and Recording Features, page 20
- LogCollectionPort Service: selectLogFiles Operation, page 21
- Perform DRS Backup After You Regenerate Certificates, page 25
- Important Information About Create File Format Capability in BAT, page 25
- Limitation Between QSIG PRI and SIP Trunk for MWI, page 25
- Cisco Unified Communications Manager Assistant Wizard Constraint, page 26
- Creating a Custom Help Desk Role and Custom Help Desk User Group, page 26
- Do Not Unplug a USB Device While It Is In Use, page 27
- Removing Hard Drives, page 27
- CSCsx96370 Multiple Tenant MWI Modes Service Parameter, page 27
- Considerations for LDAP Port Configuration, page 27
- Configuring the Hostname/IP Address for the Cisco Unified Communications Manager Server, page 28
- Adding or Updating SIP Dial Rules Causes Cisco TFTP Service to Rebuild All Phone Configuration Files, page 30
- CSCta10219 Unicast Music on Hold May Not Play, page 30
- SFTP Server Products, page 31
- CSCsu08609 Blind Transfer or Unanswered Conference Call over QSIG PRI Trunk, page 31
- Important Information About Delete Transaction by Using Custom File in BAT, page 31
- TAPS Name Change in Bulk Administration Tool, page 31

- Basic Uninterruptible Power Supply (UPS) Integration, page 32
- Strict Version Checking, page 32
- Serviceability Not Always Accessible from OS Administration, page 33
- Voice Mailbox Mask Interacts with Diversion Header, page 33
- Best Practices for Assigning Roles to Serviceability Administrators, page 33
- For Serviceability, the Administrator That Is Created During Installation Must Not Be Removed, page 33
- Connecting to Third-Party Voice Messaging Systems, page 33
- Database Replication When You Revert to an Older Product Release, page 33
- User Account Control Pop-up Window Displays During Installation of RTMT, page 34
- CiscoTSP Limitations on Windows Vista Platform, page 34
- Time Required for Disk Mirroring, page 34
- Changes to Cisco Extension Mobility After Upgrade, page 34
- RTMT Requirement When Cisco Unified Communications Manager Is Upgraded, page 34
- Serviceability Session Timeout Is Not Graceful, page 35
- Serviceability Limitations When You Modify the IP Address, page 35
- CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value, page 35
- CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters, page 35
- CSCtr84167 Block Offnet to Offnet Transfer, page 36
- CSCtr21486 Troubleshooting Guide Update for Switch Version, page 36
- MDCX Sendonly Message Suppressed for MGCP Calls, page 36
- CSCtx86215 Database Replication, page 36
- CSCti50323 Cannot delete Cisco IP Manager Assistant phone templates after upgrade from 5.X, page 36
- CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none>, page 37
- CSCtw44980 Missing Exceptions for Voice-Mail Pilot, page 37
- CSCud34740 Application User AXL Password Must Not Contain Special Characters, page 37
- CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide, page 37
- CSCud95087 Limitation of SIP Forking on Trunk Not Documented, page 38

New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651)

A new license file is required if you are installing a replacement motherboard in publisher servers or single servers that are not part of a cluster.

Limitations to Call Park Feature

The Call Park feature has the following known limitations:

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

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

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

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

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

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

CSCsz31137 Parked Call Gets Reverted When the Parkee is on

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

CSCsz35994 Incorrect Display for Park Monitoring Forward No Retrieve

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

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

CSCtb53159 Display Limitation in ConfList

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

Verify IPv6 Networking on Servers Before Upgrade

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

Node Licenses Missing After an Upgrade

If the node license file contains multiple features (for example: SW_FEATURE + CCM_NODE), after you upgrade to Cisco Unified Communications Manager 7.1(3), the following licensing warnings might display:

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

For additional details and workaround, see CSCtf15332.

CSCte56322 Netscape Browser is not Supported

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

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

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

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

Status Updates

The status of support for NAT in SCCP version 17 gets tracked by CSCsy93500. For updates, subscribe to updates in bug toolkit for CSCsy93500.

CSCtc80749 Server Boot Up Time Increases With Each Reboot and Hardware SNMP Fails

This issue exhibits two symptoms.

1. Hardware SNMP fails after reboot. Customers using hardware SNMP see the issue.
2. Server boot up time increases with each reboot. The increased length of time depends upon whether the server is an HP or IBM, but reboots up to 30 minutes might occur after 7 - 8 reboots.

Conditions

This issue exists when you upgrade to Cisco Unified CM 7.1(3) from any prior release, regardless of server model.

Note Fresh installs of Cisco Unified CM 7.1(3) are not impacted.

The server must be rebooted at least once after the upgrade to encounter this issue.

Workaround

No workaround exists for this defect. For more information, see CSCtc80749.

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

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

WorkAround

Perform the following steps:

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

Step 2 Backup your system.

Step 3 Perform a fresh installation.

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

Disaster Recovery System Caution

When you restore your data, the hostname, server IP address, and the deployment type must be the same as it was during the backup. DRS does not restore across different hostnames, IP addresses and deployment types.

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. For information on replacing a failed hard drive, refer to the *Troubleshooting Guide for Cisco Unified Communications Manager*.

CSCsx96370 Multiple Tenant MWI Modes Service Parameter

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

Be aware that this service parameter supports Cisco Unified Communications Manager integrations with Cisco Unity Connection or Cisco Unity. If your voice-mail extensions require translation in Cisco Unified Communications Manager, set the Multiple Tenant MWI Modes service parameter to **True** after you install or upgrade to Cisco Unified Communications Manager 7.1(3x).

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.)

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

Table 2 lists the locations where you can configure a host name for the Cisco Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Cisco Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

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

Table 2 Host Name Configuration in Cisco Unified Communications Manager

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

Table 2 Host Name Configuration in Cisco Unified Communications Manager

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

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

Before you configure the host name in any location in Table 2, review the following information:

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

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

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

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

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

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

Related Topics

- "Server Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*
- *Installing Cisco Unified Communications Manager, Release 7.1(2)*
- *Cisco Unified Communications Operating System Administration Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions Release 7.1(3)*
- *Changing the IP Address and Host Name for Cisco Unified Communications Manager7.1(2)*

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.

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:

Table 3 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.

CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value

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

CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters

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

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

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

CSCtr84167 Block Offnet to Offnet Transfer

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

CSCtr21486 Troubleshooting Guide Update for Switch Version

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

MDCX Sendonly Message Suppressed for MGCP Calls

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

CSCtx86215 Database Replication

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

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

CSCti50323 Cannot delete Cisco IP Manager Assistant phone templates after upgrade from 5.X

If you have upgraded from Cisco Unified Communications Manager 5.x to 7.1(3), you will be unable to delete Bulk Administration phone templates that were created with the Cisco IP Manager Assistant. Instead, you will receive the following error: "Update failed. [429] Security Profile is required for this device"

To diagnose the problem, run the following command from the command line:

```
run sql select pkid, name, tkmodel, tkdeviceprotocol, fksecurityprofile from device where
my_lower(name) in ('<template1 name>','<template2 name>','< template3 name>')
```

To fix the problem, run the following commands from the command line:

```
run sql select pkid, name from securityprofile from device where tkmodel = <model from
above> and tkdeviceprotocol = <protocol from above>

run sql update device set fksecurityprofile = '<security profile pkid from above>' where
my_lower(name) in ('<template1 name>','<template2name>', '< template3 name>')
```

CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none>

The following note is missing from the "Phone Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool.

CSCtw44980 Missing Exceptions for Voice-Mail Pilot

The following information is missing for the Voice Mail Pilot Name field description in the "Voice-Mail Pilot Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#).

CSCud34740 Application User AXL Password Must Not Contain Special Characters

The following note is missing from the Application User Settings topic in the Cisco Unified Communications Manager Administration Online Help:

Note Do not use special characters when you create an AXL password for an application user.

CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide

The *Cisco Unified Communications Manager Troubleshooting Guide* is missing the following procedure for troubleshooting if you lose all security tokens (etokens):

Perform the following procedure if you lose the security tokens and you need to update the CTL file.

Tip Perform the following procedure during a scheduled maintenance window, because you must reboot all servers in the cluster for the changes to take effect.

Step 1 On every Cisco Unified CallManager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists from the OS SSH command line.

file list tftp CTLFile.tlv

Step 2 Delete CTLFile.tlv.

file delete tftp CTLFile.tlv

Step 3 Repeat step 1 and step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 By using the Cisco CTL client, create the CTL File, as described in "Installing the Cisco CTL Client" and "Configuring the Cisco CTL Client".

Tip If the clusterwide security mode is in mixed mode, the Cisco CTL client displays the message No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click OK; then, choose Set CallManager Cluster to Mixed Mode and complete the CTL file configuration.

Step 6 Reboot all the servers in the cluster.

Step 7 After you create the CTL file on all the servers and reboot all servers in the cluster, delete the CTL file from the phone, as described in "Deleting the CTL File on the Cisco Unified IP Phone".

CSCud95087 Limitation of SIP Forking on Trunk Not Documented

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

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

New and Changed Information

This section contains information on the following topics:

- Installation, Upgrade, and Migration, page 38
- Cisco Unified Communications Operating System Administration, page 39
- Command Line Interface, page 40
- Cisco Unified Communications Manager Administration, page 41
- Cisco Unified Communications Manager Features and Applications, page 43
- Security, page 60
- Bulk Administration Tool, page 62
- Cisco Unified IP Phones, page 64

Installation, Upgrade, and Migration

This section contains information on the following topics:

- Enabling Write-Back Cache for Improved Upgrade Performance, page 39
- Maintaining Correct Time Zone Data, page 39
- Error messages display and terminal becomes unusable, page 39

Enabling Write-Back Cache for Improved Upgrade Performance

If you upgrade from Cisco Unified Communications Manager Release 7.1(3x) 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(3x) 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(3x). You do not need to upgrade Cisco Unified Communications Manager Release 7.1(3x) 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 servers in your Release 7.1(3x) cluster. (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(3x).

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

Error messages display and terminal becomes unusable

If you connect and keyboard and mouse to the server during an installation or upgrade, you must power down the server before you disconnect the keyboard and mouse. If you disconnect the keyboard and mouse while the server is powered up, the terminal displays errors and becomes unusable. To view another system without disconnecting the keyboard and mouse from the server, press ALT + <*function key*> to change the view. Function keys F1 through F6 are supported.

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(3x), page 40

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

You cannot upgrade directly from Cisco Unified Communications Manager Releases 6.0(1) or 6.1(2) to Release 7.1(3x); 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(3x)

- Commands Added, page 40
- Commands Removed, page 41

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 41
- Menu Changes, page 42
- Cisco Unified Communications Manager Features and Applications, page 43

New and Updated Enterprise and System Parameters

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

- Enterprise Parameters, page 41
- Service Parameters, page 41

Enterprise Parameters

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

Service Parameters

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

- Dial-via-Office Forward Service Access Number—See the "Cisco Unified Mobility Dial-Via-Office Forward" section on page 44.

- 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 42
- System, page 42
- Call Routing, page 42
- Media Resources, page 42
- Voice Mail, page 42
- Device, page 42
- Application, page 43
- User Management, page 43
- Bulk Administration, page 43

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 41.

Call Routing

The Call Routing menu contains no changes.

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 60.
- Device > Device Settings > Feature Control Policy—See the "Feature Control Policy in Cisco Unified Communications Manager Administration" section on page 50.

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 62.

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 43
- Cisco Unified Communications Manager Assistant Restart, page 44
- Cisco Unified Mobility Dial-Via-Office Forward, page 44
- DN Capacity Increase for the Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 49
- Enterprise Phone Configuration in Cisco Unified Communications Manager Administration, page 49
- Feature Control Policy in Cisco Unified Communications Manager Administration, page 50
- LDAP Synchronization and Authentication with Active Directory 2003 sp2 on VMWare ESX 3.5 Update 2, page 50
- Logical Partitioning Interaction with Block OffNet to OffNet Transfer Service Parameter, page 50
- Logical Partitioning Policy Tree Construction, page 52
- Logical Partitioning Policy Search Algorithm, page 53
- Redirected Dialed Number Identification Service and Diversion Header, page 53
- SIP Gateway Protocol Supports Mobile Voice Access, page 55
- Support for Microsoft Active Directory Application Mode LDAP Server, page 55

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(3x) allows synchronization from OpenLDAP 2.3.41 to the Cisco Unified Communications Manager database. In addition, Unified CM 7.1(3x) 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(3x), 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.

Cisco Unified Mobility Dial-Via-Office Forward

Release 7.1(3x) 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 45
- Dial-via-Office Forward Service Access Number, page 45
- Globalization Support for DVO-F Service Access Number, page 46
- Use Case Scenarios for Dial-via-Office Forward, page 46
- Dial-via-Office Forward Call Characteristics, page 46
- Example of Dial-via-Office Forward, page 47
- SIP Error Codes, page 47
- Dial-via-Office Forward Configuration Tips, page 47
- Dial-via-Office Forward Limitations, page 48

- Enforcement of a Single DVO-F Call per Cisco Unified Mobile Communicator Device, page 48
- Additional Documentation, page 49

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(3x) 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 46 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(3x) 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(3x) 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(3x) 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

The Enterprise Phone Configuration window in Cisco Unified Communications Manager Administration lists feature parameters that you can apply to all phones that support the parameter in the cluster. To determine whether the phone supports the feature parameter, refer to the Cisco Unified IP Phone Administration Guide that supports this version of Cisco Unified Communications Manager; for example, refer to *Cisco Unified IP Phone 6921, 6941, and 6961 Administration Guide for Cisco Unified Communications Manager 7.1 (SCCP)* or *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*.

Where to Find More Information

- Phone Administration for the Cisco Unified IP Phone 8900 and 9900 Series, page 69

Feature Control Policy in Cisco Unified Communications Manager Administration

For information on how feature control policy works, refer to the *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1(3) (SIP).*

Where to Find More Information

- Phone Administration for the Cisco Unified IP Phone 8900 and 9900 Series, page 69

LDAP Synchronization and Authentication with Active Directory 2003 sp2 on VMWare ESX 3.5 Update 2

The Cisco DirSync service in Cisco Unified Communications Manager 6.1(4) and 7.1(3x) can connect to a Windows Server Active Directory 2003 sp2 (or later) in a VMWare ESX 3.5 Update 2 (or later) session that complies with Microsoft recommended deployment guidelines for VMware ESX 3.5 Update 2. For information on deployment guidelines, refer to the Microsoft website.

After you install Active Directory 2003 sp2 (or later) on a VMWare ESX 3.5 Update 2 (or later) server, you can configure LDAP synchronization and authentication. Make sure that you activate the Cisco DirSync service in Cisco Unified Serviceability before you configure synchronization. For more information on synchronization and authentication, refer to the *Cisco Unified Communications Manager System Guide* and the *Cisco Unified Communications Manager Administration Guide*.

Ensure the following conditions are met:

- The VMWare image has 15 GB or more of hard drive space allocated.
- The OS that is being installed represents 2003.1.2a or greater; Windows 2000 does not get supported.
- The disc from which install occurs must represent either HP or IBM install disc.
- Install VMware ESX Server: 3.5.0 and follow by Windows 2003 and AD on top of it.

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 cluster that is disabled for logical partitioning retains the expected behavior that this service parameter specifies.

Logical Partitioning-Enabled Cluster

In a logical partitioning-enabled Cisco Unified Communications Manager cluster, 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(3x) 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(3x) 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 4.

Step 10 Click the **Save** button.

Table 4 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.

Table 4 LDAP Directory Configuration Settings (continued)

Field		Description
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.
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

Table 4 LDAP Directory Configuration Settings (continued)

Field		Description
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.
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.

Table 4 LDAP Directory Configuration Settings (continued)

Field	Description
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.
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 5 also get synchronized.

Table 5 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(3x), Cisco Unified Communications Manager allows Security icons to be enabled by phone model on Cisco Unified IP Phones. The Security icon indicates whether the call is secure and the connected device is trusted.

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

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

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

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

Cisco Unified Communications Manager Administration

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

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 61.

Cisco Unified IP Phones

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

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

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

Trusted Devices

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 Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971
- 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 62
- BAT Support for New Limits for Speed Dials, BLF Speed Dials, and BLF Directed Call Park, page 63
- Inserting User Device Profiles and Phones into Cisco Unified Communications Manager, page 64

Support for Feature Control Policy

The Bulk Administration GUI includes the following updates to support the feature control policy:

- Feature Control Policy drop-down list box—Choose the Feature Control Policy for this group of phones.

Note The Feature Control Policy drop-down list box displays in the Phone Template, User Device Profile (UDP) Template, and Update Phone windows.

- Insert, Export, and Validate Details support for Feature Control Policy—The following insert, export, and validate details features have support for the Feature Control Policy:
  - 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 UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Generate Phone Report

  - Generate UDP Report
- File Formats—the following file formats support the Feature Control Policy feature:
  - Phone File Format—Feature Control Policy field is a part of the Device Fields section.
  - UDP File Format—Feature Control Policy field is a part of the Device Fields section.
- Import/Export—Import/Export tool includes the following changes to support the Feature Control Policy:
  - Supports a new entity called Feature Control Policy in the Device Data section.
  - Supports Feature Control Policy field in Common Phone Profile.
  - Supports Feature Control Policy field in Phones.
  - Supports Feature Control Policy field in Device Profiles.
- BAT xlt Support for Feature Control Policy—BAT.xlt provides support for the Feature Control Policy field in the Phones, UDP, and Phones and Users sheets. You can use the BAT.xlt to add or update the Feature Control Policy field.

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 8900 and 9900 Series, page 64
- Cisco Unified IP Color Key Expansion Module, page 69
- Phone Administration for the Cisco Unified IP Phone 8900 and 9900 Series, page 69
- Cisco Unified IP Phone 6900 Series, page 71
- Secure SIP Failover for SRST, page 72
- Feature Key Capacity Increase for Cisco Unified IP Phones, page 73
- SIP Digest Authentication Name, page 74

Cisco Unified IP Phone 8900 and 9900 Series

Before you use the Cisco Unified IP Phone with Cisco Unified Communications Manager, install the latest firmware on all Cisco Unified Communications Manager servers in the cluster.

Note You can install Cisco Unified Communications Manager 7.1(3) , 7.1(3a) or 7.1(3b). After you install one of these releases, you must install Cisco Unified Communications Manager 7.1(3b)su1.

The Cisco Unified IP Phone 8900 and 9900 Series is a new and innovative portfolio of endpoints that deliver business-grade, voice communication services to customers worldwide. Three models are available:

- Cisco Unified IP Phone 8961, page 65
- Cisco Unified IP Phone 9951, page 66
- Cisco Unified IP Phone 9971, page 67

Cisco Unified IP Phone 8961

The Cisco Unified IP Phone 8961 is an advanced professional media endpoint that delivers an enhanced user experience with an easy-to-use and eco-friendly ergonomic design. Highlights of the portfolio include introduction of higher-resolution (VGA) color displays, a USB port, Gigabit Ethernet connectivity, and High-definition (HD) voice support, enabling a more productive user experience for multimedia application engagement. Application support includes XML and MIDlet-enabled applications. The Cisco Unified IP Phone 8961 is an ideal solution for knowledge professionals, administrative managers, and executives.

The Cisco Unified IP Phone 8961 supports the following features:

- Ergonomic design—The phone offers a highly usable and intuitive arrangement of lines, features, and calls. Transfer, Conference, and Hold appear on hard keys to reduce the number of presented softkeys to a maximum of 4 per call state.
- Display—The phone offers a VGA presentation for calling and applications; a 5-inch (10-cm) graphical TFT color display; 24-bit color depth; and 640 x 480 effective pixel resolution with backlighting. The display also supports localization requiring double-byte Unicode encoding for fonts.
- Ethernet—An internal 2-port Cisco Ethernet switch allows for a direct connection to a 10/100/1000BASE-T Ethernet network through an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. The system administrator can designate separate VLANs (802.1Q) for the PC and phone, providing improved security and reliability of voice and data traffic.
- USB—A USB port accelerates the usability of call handling and applications by enabling accessories such as the Cisco Unified IP Phone Color Key Expansion Module and wired headsets.
- Five programmable line/feature keys and five call session keys—The IP Phone offers five programmable line/feature keys and also provides 5 call session keys with the convenience of multiple appearances per line. This enables administrative staff to handle all activities of many sessions at the same time. Up to a maximum of 200 concurrent calls can be handled by the Cisco Unified IP Phone 8961.
- Buttons—The phone has the following buttons:
  - 5 programmable feature buttons with state-indicating LEDs
  - 5 call-session buttons with state-indicating LEDs
  - Applications, Directories, and Voicemail
  - Conference, Transfer, and Hold
  - Volume Up/Down
  - Back-lit Mute, Speakerphone, and Headset
  - Back, End Call, and 5-Way Navigation Pad
- User experience—The phone offers advanced organization of lines, speed dials, and programmable features separate from call appearances. It is ideal for those who make a few calls per day, and better for those who handle dozens of calls per hour.
- Session Initiation Protocol (SIP) Signaling—SIP interoperation with the call-control and partner applications enables a rich unified communications solution.
- Application support—XML and MIDlet-enabled applications are provided by Cisco's application development partners or customers' own development staff.

The Cisco Unified IP Phone 8961 supports the following accessories:

- IP Color Key Expansion Module—Available separately, the IP Color Key Expansion Module enables advanced use of lines, speed dials, and features, providing 36 additional line/feature keys per module. One IP Color Key Expansion Module is supported on the Cisco Unified IP Phone 8961.
- Headset support—RJ-9 and USB wired headsets.

For more information, click the following URL:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10451/ps10511/data_sheet_c78-565397.html

Cisco Unified IP Phone 9951

The Cisco Unified IP Phone 9951 is an advanced collaborative media endpoint that provides voice, applications, and accessories. Highlights include High-definition (HD) voice, a high-resolution color display, Gigabit Ethernet, and a new ergonomic design and user interface designed for simplicity and high usability. Accessories, sold separately, include a color Cisco Unified IP Color Key Expansion Module.

The Cisco Unified IP Phone 9951 supports the following features:

- Industrial design—The phone offers a highly usable and intuitive arrangement of lines, features, and calls. Transfer, Conference, and Hold appear on hard keys to reduce the number of presented softkeys to a maximum of 4 per call state.
- Display—The phone delivers VGA presentation for calling and applications, in addition to a 5-inch (10-cm) graphical TFT color display, 24-bit color depth, 640 x 480 effective pixel resolution, and backlighting. The display also supports localization requiring double-byte Unicode encoding for fonts.
- Ethernet—An internal 2-port Cisco Ethernet switch allows for a direct connection to a 10/100/1000BASE-T Ethernet network through an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. The system administrator can designate separate VLANs (802.1Q) for the PC and phone, providing improved security and reliability of voice and data traffic.
- Bluetooth—Mobility is possible for headset users within 30 feet (10 m) of their desktop, so you can go to the printer, a colleague's desk, or nearby private location while on a call.
- USB—Two USB ports increase the usability of call handling and applications by enabling accessories such as wired headsets.
- External audio ports—General-purpose audio-in and audio-out ports enable a relaxed speakerphone experience over external speakers and the microphone.
- Five lines expanding to 77 with 2 key expansion modules—The phone offers many speed dials and programmable features, so you can follow the activity of many lines. Up to 200 calls per device are supported.
- Buttons—The phone has the following buttons:
  - 5 programmable feature buttons with state-indicating LEDs
  - 5 call-session buttons with state-indicating LEDs
  - Applications, Directories, and Voicemail
  - Conference, Transfer, and Hold
  - Volume Up/Down
  - Back-lit Mute, Speakerphone, and Headset
  - Back, End Call, and 5-Way Navigation Pad

- User experience—The phone offers advanced organization of lines; speed dials and programmable features are separate from call appearances. This phone is ideal for those who make few calls per day and even those who handle dozens of calls per hour.
- Session Initiation Protocol (SIP) Signaling—SIP interoperation with the call-control and partner applications enables a rich unified communications solution.
- Application support—XML and MIDlet-enabled applications are provided by Cisco's application development partners or customers' own development staff.

The Cisco Unified IP Phone 9951 supports the following accessories:

- IP Color Key Expansion Module—Available separately, the IP Color Key Expansion Module delivers easy expansion and advanced use of lines, speed dials, and features.
- Headset support—Off-the-shelf Bluetooth and USB headsets are supported. You can use your own Bluetooth headset that you use for your cell phone or smartphone. High-definition voice analog headset support is also provided through a dedicated RJ-9 headset port on the back of the phone.

For more information, click the following URL:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10453/ps10513/data_sheet_c78-565680.html

Cisco Unified IP Phone 9971

The Cisco Unified IP Phone 9971 is an advanced collaborative media endpoint that provides voice, applications, and accessories. Highlights include high-resolution color touchscreen display, High-definition voice (HD voice), desktop Wi-Fi connectivity, Gigabit Ethernet, and a new ergonomic design and user interface designed for simplicity and high usability. Accessories, sold separately, include the Cisco Unified IP Color Key Expansion Module.

The Cisco Unified IP Phone 9971 supports the following features:

- Industrial design—The phone offers a highly usable and intuitive arrangement of lines, features, and calls. Transfer, Conference, and Hold appear on hard keys to reduce the number of presented softkeys to a maximum of 4 per call state.
- Display—The phone delivers VGA presentation for calling and applications, in addition to a 5.6-inch (14-cm) graphical TFT color touchscreen display, 24-bit color depth, 640 x 480 effective pixel resolution, and backlighting. The display also supports localization, requiring double-byte Unicode encoding for fonts.
- Ethernet—An internal 2-port Cisco Ethernet switch allows for a direct connection to a 10/100/1000BASE-T Ethernet network through an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. The system administrator can designate separate VLANs (802.1Q) for the PC and phone, providing improved security and reliability of voice and data traffic.
- Desktop Wi-Fi Ethernet—As an alternative to wired Ethernet, the phone supports an onboard Wi-Fi radio and antenna that enables connectivity to Wi-Fi access for greater return on investment (ROI) with a voice-enabled Cisco Unified Wireless Network.
- Bluetooth—Mobility is possible for headset users within 30 feet (10 m) of their desktop, so you can go to the printer, a colleague's desk, or nearby private location while on a call.
- USB—Two USB ports increase the usability of call handling and applications by enabling accessories such as wired headsets.
- External audio ports—General-purpose audio-in and audio-out ports enable a relaxed speakerphone experience over external speakers and the microphone.

- Six lines expanding to 114 with 3 key expansion modules—The phone offers many speed dials and programmable features, so you can follow the activity of many lines. Up to 200 calls per device are supported.
- Buttons—The phone has the following buttons:
  - Six feature buttons with state-indicating LEDs
  - Six call-session buttons with state-indicating LEDs
  - Applications, Directories, and Voicemail
  - Conference, Transfer, and Hold
  - Volume Up/Down
  - Back-lit Mute, Speakerphone, and Headset
  - Back, End Call, and 5-Way Navigation Pad
- User experience—The phone offers advanced organization of lines; speed dials and programmable features are separate from call appearances. This phone is ideal for those who make few calls per day and even those who handle dozens of calls per hour.
- Session Initiation Protocol (SIP) Signaling—SIP interoperation with the call-control and partner applications enables a rich unified communications solution.
- Application support—XML and MIDlet-enabled applications are provided by Cisco's application development partners or customers' own development staff.

The Cisco Unified IP Phone 9971 supports the following accessories:

- IP Color Key Expansion Module—Available separately, the IP Color Key Expansion Module delivers easy expansion and advanced use of lines, speed dials, and features.
- Headset support—Off-the-shelf Bluetooth and USB headsets are supported. You can use your own Bluetooth headset that you use for your cell phone or smartphone. High-definition voice analog headset support is also provided through a dedicated RJ-9 headset port on the back of the phone.

For more information, click the following URL:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10453/ps10512/data_sheet_c78-565717.html

Requirements

The Cisco Unified IP Phone 8900 and 9900 require the following releases:

- Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition Versions 7.1(3) and later using Session Initiation Protocol (SIP).
- Cisco IP Phone Firmware release 9.0(1) or later.

Where to Find More Information

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*
- *Cisco Unified IP Phone 9971 Quick Start for Administrative Assistants*
- *Cisco Unified IP Phone 9971 Quick Start for Executives*
- *Cisco Unified IP Phone 9951 and 8961 Quick Start for Administrative Assistants*
- *Cisco Unified IP Phone 9961 and 8961 Quick Start*

Cisco Unified IP Color Key Expansion Module

The Cisco Unified IP Color Key Expansion Module delivers affordable and scalable expansion of line/feature key appearances on Cisco Unified IP Phone 9900 Series and Cisco Unified IP Phone 8900 Series endpoints.

The Cisco Unified IP Color Key Expansion Module supports the following features:

- Intended for use by manager, executives, and administrative staff
- 18 physical, programmable, tri-color illuminated LED line/ feature keys per module reduce costs versus provisioning additional phones
- Second page key provides access to 18 additional programmable keys (for 36 keys total per module) delivering superior scalability
- Tri-color LED illuminated line/feature keys provide at-a-glance call status indication
- One-, two-, and three-module configurations expand scalability and provide investment protection
- Graphical, backlit, high-resolution color display makes viewing easy
- Elegant and clean ergonomic design seamlessly integrates with Cisco Unified IP Phone 9971, 9951, and 8961
- Eco-friendly features:
  - Deep-Sleep option reduces power consumption in off-hours over the module in active state during the day
  - Uses reground and recyclable plastics

Requirements

The Cisco Unified IP Color Key Expansion Module requires the following releases:

- Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition Versions 7.1(3) and later using Session Initiation Protocol (SIP).
- Cisco IP Phone Firmware release 9.0(1) or later.

Where to Find More Information

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*

Phone Administration for the Cisco Unified IP Phone 8900 and 9900 Series

The following Cisco Unified IP Phones are supported with this release of Cisco Unified Communications Manager:

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

Features that the Cisco Unified IP Phone 8961, 9951, and 9971 support include:

- Park monitoring—Monitors the status of a call after the call has been parked.
- Assisted directed call park—Lets the end user press only one button to direct-park a call.

- Feature control policies—Allows the administrator to limit the appearance of features on the Cisco Unified IP Phone 8961, 9951, and 9971 by disabling them in Cisco Unified Communications Manager administration.
- Cisco Unified IP Color Key Expansion Module—Attaches to your Cisco Unified IP Phone 8961, Cisco Unified IP Phone 9951, and Cisco Unified IP Phone 9971 to add additional line appearances or programmable buttons to your phone.

  You can add one Key Expansion Module (KEM) to the Cisco Unified IP Phone 8961 to add up to 36 extra lines or buttons, two Expansion Modules to the Cisco Unified Phone 9951 to add up to 72 extra lines or buttons, and three Expansion Modules to the Cisco Unified IP Phone 9971 to add up to 108 extra lines or buttons. Table 6 includes a graphical representation of KEM support by phone.
- Softkey templates not used—The Cisco Unified IP Phone 8961, 9951, and 9971 do not use softkey templates. Features are available either on softkeys, dedicated feature buttons, or as programmable feature buttons configured by the system administrator.
- Product-specific configuration—Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco Unified IP Phones in any of the following windows:
  - Phone Configuration window (**Device > Phone**); Product Specific Configuration portion of window
  - Common Phone Profile window (**Device > Device Settings > Common Phone Profile**)
  - Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**)
- Accessory support—Table 6 indicates the accessories that the Cisco Unified IP Phones 8961, 9951, and 9971 support; an "X" indicates support for a particular phone model and a dash (—) indicates non-support:

Table 6 Accessory Support for the Cisco Unified IP Phone 8961, 9951, and 9971

Accessory	Type	Cisco Unified IP Phone		
		8961	9951	9971
Cisco Accessory				
Cisco Unified IP Color Key Expansion Module	Add-on module	1	up to 2	up to 3
Third-Party Accessories				
Headsets—	Analog	X	X	X
	Analog Wideband	X	X	X
	Bluetooth	—	X	X
	USB	X	X	X
Microphone	External PC	—	X	X
Speakers	External PC	—	X	X

For configuration information about these features, and other information about administering the Cisco Unified IP Phone 8961, 9951, and 9971, see the *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1(3) (SIP)*, at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/9971_9951_8961/7_1_3/english/admin/guide/8961995171_713_ag.html

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 7 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 8 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.1(3x) Features

Cisco Unified Communications Manager 7.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Cisco Unified IP Phone 8900 and 9900 Series	SIP only 8961 9951 9971	Cisco Unified IP Phone 8900 and 9900 Series, page 64
Cisco Unified IP Phone 6900 Series	SCCP only 6921 6941 6961	Cisco Unified IP Phone 6900 Series, page 71
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 72
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 73 DN Capacity Increase for the Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 49
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 74

Cisco Unified Serviceability and RTMT

This section contains information on the following topics:

- Feature Control Policy Support in RTMT and Cisco Unified Serviceability, page 76

Feature Control Policy Support in RTMT and Cisco Unified Serviceability

Performance monitor counters display in RTMT for feature control policy. The following Cisco TFTP counters support feature control policy:

- BuildFeaturePolicyCount—Indicates the number of files built for feature control policy.
- FeaturePolicyChangeNotifications—Indicates the number of change notifications for feature control policy.

Updated TFTP alarms exist in Cisco Unified Serviceability to support feature control policy. The following alarm values exist for the BuildStat alarm in the TFTPAlarm Catalog (System > TFTP Alarm Catalog):

- FeatureControlPolicyCount—Indicates the number of files built for feature control policy.
- FeatureControlPolicyTime—Indicates the time it takes to build the files for the feature control policy.

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(3b) As of December 11, 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(3b) As of December 11, 2009" section on page 78 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.

- 7.1(3.20000-x) = Cisco Unified Communications Manager Release 7.1(3a)

- 7.1(3.10000-11) = Cisco Unified Communications Manager Release 7.1(3)
- 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(3b) As of December 11, 2009" section on page 78 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 76.

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(3b) As of December 11, 2009

The following information comprises unexpected behavior (as of December 11, 2009) that you may encounter in Release 7.1(3b) of Cisco Unified Communications Manager.

Table 9 Open Caveats for Cisco Unified Communications Manager 7.1(3b) as of December 11, 2009

Id	Component	Headline
CSCtd78306	bps-bat	BAT does not modify SNMP configuration settings for Telepresence device.
CSCtd65993	cm-docs	need modification in cucm 7.x docs to mention CSCsy93500 for NAT interop
CSCsr30432	cmcti	c2conf: Cisco Unified CM does not send NOTIFY.
CSCsx68761	cmcti	Duplicate callPartyInfoChangedEvent exists party gets dropped across cluster.
CSCtd74238	cmcti	CTIERR_TIMEOUT for CallRetrievereq
CSCtb80964	cmcti	Race condition caused by remote access connection does not get handled properly.
CSCtd72314	cmcti	CTIManager cores when LDAP authentication fails.
CSCtc48317	cmcti	Intermittently, CTI-enabled line cannot be controlled by using the TSP application.
CSCtd50757	cmui	User//Phone Add creates user that cannot be imported to UnityConnection.

CSCtd69700	cp-digit-analysis	Translation pattern waits for interdigit timer.
CSCsy62649	cp-mediacontrol	sRTP: Call drops after a sequnce of blind and supervised transfers.
CSCtd16828	cp-mediacontrol	No video in hairpin conference involving Round Table video and polycom.
CSCtd20045	cp-mediacontrol	No video between polycom and CUVA on SIP hairpin call.
CSCtd17335	cp-mediacontrol	Video lost on hairpin sTransfer call with RT video after hold/resume.
CSCtd63304	cp-mediacontrol	H.239 breaks when an intra-cluster call leg exists.
CSCtd17128	cp-sip-trunk	Polycom initiated call to TB displays no video.
CSCtc68789	cpi-appinstall	No Unrestricted for Console Screen after installation.
CSCtc91574	cpi-os	Unified CM h7.1.2 SNMP agent gives other(1) status for cpqHeFltTolFanCondition
CSCtd73461	cpi-os	Platform CLI **show hardware** does not show battery status on IBM servers.
CSCtc99277	cpi-os	Upgrade NTPd used within Cisco Unified CM.
CSCtb92903	cpi-os	RTMT log collection batch command process executed during sftp hangs
CSCtb83367	cpi-os	/usr/bin/script generates core
CSCtd01282	cpi-third-party	IMPORTANT TLS/SSL SECURITY UPDATE - OpenSSL
CSCtb66354	cpi-vendor	IBM Director Agent reports defunct drive - false RAID alert
CSCtc22869	database	Control-C for "show tech database dump" causes server to stop functioning.
CSCtd63152	database	Database audit logs leads to LPM HWM when log rotation is enabled.
CSCtd31555	database	User Facing Feature data changes get lost when publisher server gets rebuilt
CSCtc36390	database-ids	PMR 09825: Assert Fail, mtex.c Line: 458
CSCtd31951	database-ids	PMR 18554 cdr check is hung after DRS Restore of Publisher
CSCtd74762	ext-mobility	Webdialer does not work with EM when App User has '&' in password.
CSCtd70266	ipma-service	IPMA:Manager's intercom does not automatically point to active assistant
CSCtd14027	security	IMPORTANT TLS/SSL SECURITY UPDATE - JDK
CSCtd14040	security	IMPORTANT TLS/SSL SECURITY UPDATE - RSA

Documentation Updates

Documentation Updates

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

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