Release Notes for Cisco Unified Communications Manager Release 7.1(2a)

Published June 15, 2009

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

This document contains information pertinent to Cisco Unified Communications Manager Release 7.1(2) (which is deferred) as well as information specific to Cisco Unified CM 7.1(2a).

To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the "Important Notes" section on page 11 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(2a).

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your

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

system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the "The Latest Software Upgrades for Unified CM 7.1 on Cisco.com" section on page 11.

Introduction

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

System Requirements

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

Server Support

Make sure that you install and configure Cisco Unified CM on a Cisco Media Convergence Server (MCS) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS are compatible with this release of Cisco Unified CM, refer to the Supported Servers for Cisco Unified Communications Manager Releases: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.

Note Make sure that the matrix shows that your server model supports Cisco Unified CM Release 7.1(2a).

Note Be aware that some servers that are listed in the *Cisco Unified Communications Manager Software Compatibility Matrix* may require additional hardware support for Cisco Unified CM Release 7.1(2a). 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 in order to prevent file system corruption during power outages.

When Cisco Unified Communications Manager runs on one of the servers 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 show ups status CLI command which 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 once 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-7828-I3
	MCS-7828-I4
	MCS-7828-I4
	MCS-7835-I1
	MCS-7835I-30
	MCS-7845-I2

Upgrading to Cisco Unified Communications Manager 7.1(2a)

The following sections contain information 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(2a), page 9
- Ordering the Upgrade Media, 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.

Special Upgrade Information

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

I/O throttling

This section describes how I/O throttling affects the upgrade process, identifies possible causes of slow or stalled upgrades, and provides actions you can take to speed up the upgrade.

I/O throttling Overview

I/O throttling prevents call processing degradation during the upgrade but may cause the upgrade to take longer. I/O throttling gets enabled by default and is necessary if you perform the upgrade during normal business hours. Be aware that the higher the call processing load on the system during the upgrade, the longer the upgrade takes.

Disabling I/O throttling

If you can perform the upgrade during a maintenance window, you can disable I/O throttling to decrease the time that it takes for the upgrade to complete.

To disable I/O throttling, use one of the following methods before you start the upgrade:

- To disable I/O throttling in Cisco Unified Operating System Administration, choose **Software Upgrades > Install/Upgrade**, and check the Disable I/O throttling checkbox.
- To disable I/O throttling from the command line interface (CLI) use the **utils iothrottle disable** command.

Note If call traffic exists on the system with I/O throttling disabled, the system may become overloaded and deny new calls. In the worst case, the Cisco CallManager service might restart; however, existing calls get preserved if the Cisco CallManager service restarts.

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

Server Models

The server model that you have also impacts the upgrade speed. Upgrades on servers that have SATA hard drives, such as MCS-7816, MCS-7825, MCS-7828, take longer than servers with SAS/SCSI hard drives, such as MCS-7835 and MCS-7845.

Write-Cache

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

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 1-1 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 1-2 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(2a) Upgrade

Before you upgrade to Cisco Unified Communications Manager 7.1(2a), 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(2a) 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(2a)

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(2a), 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. This COP file is available from 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 included with the COP file.

Upgrading from Unified CM 6.1(2) or Later to Unified CM 7.1(2a) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_7.1.2.20000-2.sgn.iso, comprises two parts:

- UCSInstall_UCOS_7.1.2.20000-2.sgn.iso_part1of2
- UCSInstall_UCOS_7.1.2.20000-2.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 7.1.2.20000-2 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_7.1.2.20000-2.sgn.iso_part1of2 UCSInstall_UCOS_7.1.2.20000-2.sgn.iso_part2of2 > UCSInstall_UCOS_7.1.2.20000-2.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_7.1.2.20000-2.sgn.iso_part1of2+UCSInstall_UCOS_7.1.2.20000-2.sgn.iso_part2of2 UCSInstall_UCOS_7.1.2.20000-2.sgn.iso
```

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

4b9836cd8c29d02c90dd5f9bd8863f16 UCSInstall_UCOS_7.1.2.20000-2.sgn.iso

Step 4 Create a non-bootable DVD that contains the files necessary for the upgrade.

Consider the following:

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

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

Upgrading From an Engineering Special

If you want to upgrade to Cisco Unified CM 7.1(2a) and you are currently running an Engineering Special (ES), contact TAC to obtain the fixes that are included in the ES that you currently use.

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

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

Related Documentation

The view documentation that supports Cisco Unified CM Release 7.1(2a), 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(2a) 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(2a). 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(2a).

- CSCta09513 Switch Version Does Not Complete, page 12
- CSCta12062 Null Value in NetworkLocale Caused Database Exception, page 12
- CSCsz91530 Logical Partitioning Feature Does Not Work Correctly in Conference Scenario When Multiple H.323 Gateways Are Configured in a Route Group, page 12
- CSCsy92863 Intercom Route Partition Online Help Is Incorrect, page 13
- Admin Password Gets Corrupted If Correction is Made During Password Reset, page 13

CSCta09513 Switch Version Does Not Complete

Prior to the release of Cisco Unified Communications Manager Release 7.1(2a), if your servers were running Cisco Unity Connection 2.x and you attempt to upgrade to Cisco Unified CM 7.1(2), the switch version task did not complete to make the new version software the active partition.

The release of Cisco Unified CM 7.1(2a) resolves this problem.

CSCta12062 Null Value in NetworkLocale Caused Database Exception

Prior to Cisco Unified Communications Manager Release 7.1(2), AXL did not allow a tkField to get updated to NULL. When an EMPTY value was sent in tags (for example, <networkLocale></networkLocale> in the UpdatePhone API), the EMPTY value was ignored.

Cisco Unified CM 7.1(2) included a change to this behavior. EMPTY values did not get ignored. They updated the database with a NULL value.

This behavioral change caused applications that send EMPTY values in ENUM tags in their insert operations to fail.

The release of Cisco Unified CM Release 7.1(2a) restores the original behavior. EMPTY tkFields get ignored.

CSCsz91530 Logical Partitioning Feature Does Not Work Correctly in Conference Scenario When Multiple H.323 Gateways Are Configured in a Route Group

The logical partitioning feature does not work as defined in the *Cisco Unified Communication Manager Administration Guide* under the following conditions:

Conditions

- Enterprise parameter, logical partitioning feature is enabled.
- A single route group gets configured with multiple H.323 gateways

  or

  A route group gets configured with an H.323 gateway in combination with another MGCP port/SIP trunk device.

Effect

Be aware that, under these conditions, when a call gets routed to the H.323 gateway, the geolocation that corresponds to the call is not available for logical partitioning policy matching.

Workaround

To ensure that you do not encounter this caveat, either

- Configure the route group with a single H.323 gateway.
- Configure the route group with MGCP gateways/ports or SIP trunks (with no limitation on number or combinations).

For more information see CSCsz91530.

CSCsy92863 Intercom Route Partition Online Help Is Incorrect

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

Admin Password Gets Corrupted If Correction is Made During Password Reset

When you use the Pwrecovery tool to reset your password, if the new password is unacceptable, one of the following messages displays.

- Passwords do not match.

  This message displays if, when you attempted to change the password, you did not enter exactly the same word when you confirmed the new password.
- Password too short.

  This message displays if the password that you entered is fewer than 6 characters.
- Password in dictionary.

  This message displays if the password that you entered already exists in the dictionary or is based on a word that already exists in the dictionary.

If you continue by entering an acceptable password, the system seems to accept the reset password; however, that password cannot be used and attempts to use pwrecovery do not work. GUI log in still works, but you cannot log into the platform GUI or CLI.

Workarounds

- Passwords Do Not Match, page 13
- Password Too Short or Password in Dictionary, page 14

Passwords Do Not Match

Log in as pwrecovery to relaunch the pwrecovery tool and follow normal procedure.

Password Too Short or Password in Dictionary

Contact TAC to reset the admin password.

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*.

CSCsz33878 IPMA Wizard Constraint

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

CSCsz21235 Core Dump File Gets Generated During the Cisco Security Agent Shutdown Process

Intermittently, your system may experience a core dump during the Cisco Security Agent for Unified Communications Manager shutdown process.

Cause

Causes of the core dump include

- Use of the CLI command **utils disable csa**, which disables Security Agent for Unified CM.
- Use of the following CLI commands that shut down Security Agent for Unified CM:
  - **utils system restart**
  - **utils system shutdown**
  - **utils system switch-version**
  - **utils system upgrade**
- During an upgrade, Security Agent for Unified CM shuts down and may cause the core dump file to get generated.

Workaround

No workaround exists. You initiated an action that required Security Agent for Unified CM to shut down. Security Agent for Unified CM will shut down properly, but might leave a core file as a result of the shutdown operation.

The core file gets generated infrequently. This defect does not introduce any security concern and does not impact call processing as it is only encountered after a user-initiated action that requires Security Agent for Unified CM to be shut down.

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*.

Use Microsoft Outlook to Receive Cisco Unified Communications Manager Licenses

When you obtain a license file from the Product License Registration window on www.cisco.com, the system sends the license file(s) to you via e-mail by using the e-mail ID that you provided. When you receive license files from e-mail clients other than Microsoft Outlook, for example, Microsoft Entourage, additional characters may exist in the license file, which can prevent you from being able to upload the license file in Cisco Unified Communications Manager Administration. To avoid this issue, Cisco recommends that you use Microsoft Outlook when you receive license files for Cisco Unified Communications Manager.

If you obtained a license file with additional characters in it, perform the following procedure:

Procedure

Step 1 Use the CLI to delete the license file from the Cisco Unified Communications Manager server. In the CLI, run the command, **file delete license <name of license file>**.

Step 2 Restart the Cisco License Manager service in Cisco Unified Serviceability.

Step 3 Use Microsoft Outlook to save the received license file.

Step 4 In Cisco Unified Communications Manager Administration, upload the saved license file, as described in the “Uploading a License File” section of the *Cisco Unified Communications Manager Administration Guide*.

For More Information

- “Licensing” chapter, *Cisco Unified Communications Manager System Guide*

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(2).

New and Changed Information

This section contains information on the following topics:

Documentation Changes

This section highlights some documentation changes for the 7.1(2) release; for example, this section highlights new documents, new chapters in guides, and information that moved from one document to another document. This section does not contain all the documentation updates for the 7.1(2) release. Use this section in conjunction with the information in the "New and Changed Information" section and the "Documentation Updates" section.

Cisco Unified Communications Manager Administration Updates

- In the *Cisco Unified Communications Manager Features and Services Guide* and the *Cisco Unified Communications Manager System Guide*, the configuration checklists now display at the beginning of the chapters.
- In the *Cisco Unified Communications Manager Administration Guide*, the configuration settings tables now display at the beginning of the chapters.
- In previous releases, the information on configuring the intercom route partition, intercom calling search space, intercom directory number, and intercom translation pattern displayed in the *Cisco Unified Communications Manager Administration Guide*. This configuration information now exists in the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

  Troubleshooting information for intercom now exists in the *Troubleshooting Guide for Cisco Unified Communications Manager*, instead of in the "Intercom" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.
- In previous releases, the information on configuring device mobility groups and device mobility info displayed in the *Cisco Unified Communications Manager Administration Guide*. This configuration information now exists in the "Device Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

- The *Cisco Unified Communications Manager Features and Services Guide* contains a new chapter, “Internet Protocol Version 6 (IPv6).” For information on configuring IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 64 and the new chapter.
- The *Cisco Unified Communications Manager Features and Services Guide* contains a new chapter, “Geolocations and Location Conveyance.” For information on configuring geolocations, geolocation filters, and location conveyance, see the “Geolocations, Geolocation Filters, and Location Conveyance” section on page 50 and the new chapter.
- The *Cisco Unified Communications Manager Features and Services Guide* contains a new chapter, “Logical Partitioning.” For information on configuring logical partitioning, see the “Logical Partitioning” section on page 110 and the new chapter.
- The Release 7.0(1) version of the “Cisco Unified Mobility” chapter of the *Cisco Unified Communications Manager Features and Services Guide* included information about all Cisco Unified Mobility features, including Cisco Unified Mobility features and capabilities that are native to Cisco Unified Communications Manager and require configuration entirely within Cisco Unified Communications Manager Administration, as well as Cisco Unified Mobility features and capabilities that require configuration of both Cisco Unified Communications Manager Administration and also Cisco Unified Mobility Advantage.

  The Release 7.1(2) version of the “Cisco Unified Mobility” chapter of the *Cisco Unified Communications Manager Features and Services Guide* includes only the Cisco Unified Mobility features and capabilities that are native to Cisco Unified Communications Manager.

  The Cisco Unified Mobility features and capabilities that require configuration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator now get documented in the new chapter, “Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration,” of the *Cisco Unified Communications Manager Features and Services Guide*. The “Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration” chapter discusses the following topics:

  - Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage
  - Introducing Cisco Unified Mobility with Cisco Unified Mobility Advantage, including the following topics—Definitions, List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage, and Cisco Unified Mobile Communicator, Dial-via-Office Reverse Callback
  - Use Case Scenarios for Cisco Unified Mobility Features
  - Interactions and Restrictions
  - System Requirements
  - Configuring Cisco Unified Mobility with Cisco Unified Mobility Advantage

Serviceability Updates

- In previous releases, the *Cisco Unified Serviceability Administration Guide* contained the “SNMP Troubleshooting” chapter. This chapter now exists in the *Troubleshooting Guide for Cisco Unified Communications Manager*.
- The *Cisco Unified Serviceability Administration Guide* contains a new chapter, “Configuring the Audit Log.” For information on configuring the audit log, see the “Audit Logging” section on page 155 and the new chapter.
- With Cisco Unified Communications Manager, Release 7.1(2), a new documentation guide for Managed Service Providers, *Cisco Unified Communications Manager Managed Services Guide, Release 7.1*, contains the following information:

  - New and changed information for Cisco Unified Communications Manager, release-to-release, beginning with 6.0(x).
  - Managing and monitoring the health of Cisco Unified Communications Manager Systems including an overview of supported interfaces, hardware platform monitoring, RTMT monitoring of Cisco Unified Communications Manager system health, and critical processes to monitor.
  - Overview of the Simple Network Management Protocol, including SNMP tips, troubleshooting, and SNMP/R MIBs.
  - Cisco Unified Real-Time Monitoring Tool Tracing, PerfMon, and Alerts chapter describing trace tools and collection, trace field descriptions, and performance monitoring.
  - Cisco Unified Serviceability Alarms and CiscoLog Messages that include descriptions, application names, facility/subfacility headers, corrective actions, level of severity.
  - Applicable Cisco MIBs, including CISCO-CCM-MIB.
  - Applicable industry-standard MIBs, including HOST-RESOURCES-MIB.
  - Applicable vendor-specific MIBs, including a list of Cisco-supported servers and MIBs for HP, Intel, and IBM.

Installation, Upgrade, and Migration

This following sections describe the changes for installation, upgrade, and migration in Cisco Unified Communications Manager 7.1(2):

- System History Log for Cisco Unified Communications Manager, page 19
- Data Migration Assistant (DMA), page 22
- Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(2) Upgrade, page 23

System History Log for Cisco Unified Communications Manager

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, DRS backups and DRS restores, as well as switch version and reboot history.

Description

This section provides a description of the system history log feature.

Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data does not get maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success and failure of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.

- Logs every invocation of Switch Version, issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown, issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot occurs as the result of a manual reboot, power cycle, or kernel panic.
- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. You can access the log from the CLI by using the **file** commands and by using the Real Time Monitoring Tool (RTMT).

System History Log Fields

Each system history log entry contains the following fields:

- <*timestamp*> <*userid*> <*action*> <*description*> <*start/result*>

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- action—Displays one of the following actions:
  - Basic Install
  - Windows Upgrade
  - Upgrade During Install
  - Upgrade
  - Cisco Option Install
  - Switch Version
  - System Restart
  - Shutdown
  - Boot
  - DRS Backup
  - DRS Restore
- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, Windows Upgrade, Upgrade During Install, Upgrade, and ServerPak Install actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.
  - *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
  - *Active version to inactive version*: Displays for the Switch Version action.
  - *Active version*: Displays for the System Restart, Shutdown, and Boot actions.
- result—Displays the following results:
  - Start
  - Success or Failure
  - Cancel

Example

Example 3 shows a sample of the system history log.

Example 3 System History Log

```
admin:file dump install system-history.log
=======================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
=======================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start
07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success
07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

CLI Considerations

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

Cisco Unified Communications Manager Administration Configuration Tips

No Cisco Unified Communications Manager Administration configuration tips exist for this feature.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service parameter and enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade considerations exist for this feature.

Serviceability Considerations

To access the system history log in RTMT, navigate to RTMT Trace Collection:

RTMT > Trace Log Collection

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

For More Information

For more information about using the CLI, see the *Cisco Unified Communications Operating System Administration Guide* or the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For more information about RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Data Migration Assistant (DMA)

Cisco Unified Communications Manager Release 7.1(2) includes the following Data Migration Assistant (DMA) enhancements. For more details, refer to the documents *Data Migration Assistant User Guide 7.1(2)* and *Upgrading to Cisco Unified Communications Manager Release 7.1(2) from 4.x Releases*:

- The platformConfig.xml file that is generated by DMA supports upgrades for the first node (publisher database server) as well as for the subsequent nodes (subscribers). DMA provides a window where you can make detailed configuration specifications. Enter data at the DMA window Export > Answer File Generator.
- DMA provides a window where users can customize the behavior of DMA, by specifying which types of logs to include in the output file. Enter data at the DMA window Export > Custom Options.
- DMA explicitly lists the pre-DMA export tasks. DMA provides both information and the automation of pre-export tasks, when possible, to ensure that you know what tasks you need to complete before running DMA. Enter data at the DMA window Export > Pre-Export Tasks.
- DMA supports the generation of a license file upon successful DMA validation. Go to the DMA window Export > Storage Location and specify a local directory destination for the license file licupgrade.lic Specify the destination in the “Path Name” text box of the “Destination Option for License File” field.
- DMA displays the latest timestamp of the CDR and CAR data. If these timestamps do not match, DMA displays a message that indicates that users must load the latest CDR records into the CAR database for the records to be exported.
- DMA enhances pre-upgrade instructions with regard to the CAR database. DMA displays information from the CAR database, including current number of CAR records, start date, and end date, so users can determine how many records exist and how many records that DMA can export.
- DMA provides options on how to handle CAR data during the DMA export process. The default option specifies that DMA does not export the CAR database. If you want to have this data included in the DMA TAR file, you must choose to include the CAR records in the DMA TAR file. DMA indicates the time (in 30 minute intervals) that DMA requires to migrate the CAR data. DMA displays the approximate number of records that are migrated during this time as well as the total number of CAR records on the server.

DMA does not support manual removal of the C:\DMARoot folder. If the folder is removed during the export process, DMA generates an error.

Allow as much time as possible—preferably several weeks—between the completion of your Data Migration Assistant backup and the beginning of your upgrade to Cisco Unified Communications Manager Release 7.1(2).

For More Information

- Upgrade of CAR Data, page 168

Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(2) Upgrade

For information on this topic, see the "Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters Before 7.1(2a) Upgrade" section on page 7.

Cisco Unified Communications Operating System Administration

This section describes changes to the Cisco Unified Communications Operating System Administration GUI.

- Customized Log-on Message, page 23
- Ethernet IPv6 Configuration Settings, page 24

Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified Communications Manager Administration, and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades > Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10 KB.

When you next log in to the system, the customized log-on message displays.

Step 4 To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

Ethernet IPv6 Configuration Settings

Use the following procedure to enable and configure IPv6 on the server.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings > IP > Ethernet IPv6**.

The Ethernet IPv6 Configuration window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see Table 2.

Step 3 To preserve your changes, click **Save**.

Note If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, you must reboot the system.

Table 2 Ethernet IPv6 Configuration Fields and Descriptions

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the server.
Address Source	Choose one of the following IP address sources: • Router Advertisement • DHCP • Manual Entry Be aware that the three IP address sources are mutually exclusive. **Note** Unless you specify **Manual Entry**, the IP Address and Mask fields remain read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the server; for example: fd6:2:6:96:21e:bff:fecc:2e3a
IPv6 Mask	If you chose Manual Entry, enter the IPv6 mask; for example: 64
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** For the IPv6 settings to take effect, you must reboot the system.

For More Information

- Internet Protocol Version 6 (IPv6), page 64

Command Line Interface

This section contains information about the Command Line Interface (CLI).

- show memory, page 25
- Spaces in File Names, page 25
- Relative Paths, page 25
- New Commands and Parameters, page 26

show memory

The *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 6.1(3)* does not contain updated information for the show memory command. Use the following updated information.

Command Syntax

show memory

count

modules

size

Options

- **count**—Displays the number of memory modules on the system.
- **modules**—Displays detailed information about all the memory modules.
- **size**—Displays the total amount of memory.

Parameters

None

Spaces in File Names

You can use CLI commands to directly work with file names that contain spaces. For example, you could use the **file delete** command to delete a log file with the name cisco test log in the Platform directory:

file delete activelog platform cisco test log

Relative Paths

When you download a file to your local computer with the **file get** command, the system prompts you to enter a download directory. You can specify a relative path for the download directory by using the **./** notation, as shown in the following example:

Download directory: ./RepStat

If you specify a download directory that does not exist on your local computer, the **file get** command creates it for you.

New Commands and Parameters

This section provides information about the new CLI commands for Cisco Unified Communications Manager Release 7.1(2).

For more information about command syntax and parameters, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

- **utils auditd {enable|disable|status}**

  This command enables, disables, and provides the status of audit logging. When audit logging is enabled, the system monitors and records user actions in both Cisco Unified Communications Manager and Cisco Unified Serviceability.

  You can also use the CLI **file** commands to manipulate the audit log, including the following commands:

  - **file list activelog audit**
  - **file view activelog audit** <filename>
  - **file dump activelog audit** <filename>
  - **file get activelog audit** <filename>
  - **file search activelog audit** <filename>

Note Cisco recommends that you retrieve the audit log by using the Cisco Unified Real-Time Monitoring Tool.

- **utils create report csa**

  This command collects all the files that are required for CSA diagnostics and assembles them into a single CSA diagnostics file. You can retrieve this file by using the **file get** command.

- **set password complexity character {enable|disable}**

  Use this command to enable password complexity rules for the type of characters in a password.

  When you enable password complexity, you must follow these guidelines when you assign a password:

  - It must have at least one lower-case character.
  - It must have at least one uppercase, one digit, and one special character.
  - You cannot use adjacent characters on the keyboard.
  - You cannot reuse any of the previous 10 passwords.
  - You can change the admin user password only once in 24 hours.

- **set password complexity minimum-length**

Note Use this command only after you enable password character complexity.

  Use this command to modify the value for the minimum password length for Cisco Unified Communications Operating System accounts.

Acceptable values must be equal-to or greater-than 6.

- **set password age maximum**

  Use this command to modify the value for maximum password age, in days, for Cisco Unified Communications Operating System accounts.

  Be aware that acceptable values must be equal-to or greater-than 90 days.

In the Command Line Interface, the system supports the following commands that are related to enabling and configuring IPv6:

- **set network ipv6**

  This command enables IPv6 and sets system and network options.

- **show network ipv6**

  This command displays IPv6 network routes and network settings.

- **utils network ipv6 firewall**

  This command sets options and displays status for the IPv6 network firewall.

- **utils network ipv6 host**

  This command does an IPv6 host lookup (or IPv6 address lookup) for the specified host name or IPv6 address.

- **utils network ipv6 ping**

  This command allows you to ping an IPv6 address or hostname.

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

- New and Updated Enterprise and System Parameters, page 27
- Menu Changes, page 29
- Cisco Unified Communications Manager Features and Applications, page 32

New and Updated Enterprise and System Parameters

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

- Enterprise Parameters, page 27
- Service Parameters, page 28

Enterprise Parameters

To access the enterprise parameters in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. To display the help for the service parameter, click the name of the enterprise parameter in the window.

- Enable IPv6—See the "Internet Protocol Version 6 (IPv6)" section on page 64.
- IP Addressing Mode Preference for Media—See the "Internet Protocol Version 6 (IPv6)" section on page 64.
- IP Addressing Mode Preference for Signaling—See the "Internet Protocol Version 6 (IPv6)" section on page 64.

- Allow Auto-Configuration for Phones—See the "Internet Protocol Version 6 (IPv6)" section on page 64.
- Enable Logical Partitioning—See the "Logical Partitioning" section on page 110.
- Default Geolocation—See the "Logical Partitioning" section on page 110.
- Logical Partitioning Default Policy—See the "Logical Partitioning" section on page 110.
- Logical Partitioning Default Filter—See the "Logical Partitioning" section on page 110.

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.

- Party Entrance Tone—This parameter supports the Cisco CallManager service for the Viewing Held Calls on Shared Lines feature.
- Always Use Prime Line—This parameter supports the Cisco CallManager service for the Always Use Prime Line feature.
- Always Use Prime Line for Voice Message—This parameter supports the Cisco CallManager service for the Always Use Prime Line for Voice Message feature.
- Table Out Of Sync—This parameter supports the Cisco CallManager service for the Table Out of Sync Detection feature.
- Send Multicast MOH in H.245 OLC Message—This parameter supports the Cisco CallManager service for the Multicast Music On Hold Over H.323 Intercluster Trunks feature.
- Call Counting CAC Enabled—This parameter supports the Cisco CallManager service for the Internet Protocol Version 6 (IPv6) feature.
- Audio Bandwidth For Call Counting CAC—This parameter supports the Cisco CallManager service for the Internet Protocol Version 6 (IPv6) feature.
- Video Bandwidth For Call Counting CAC—This parameter supports the Cisco CallManager service for the Internet Protocol Version 6 (IPv6) feature.
- Alternate Cisco File Server(s)—This parameter supports the Cisco TFTP service for the Internet Protocol Version 6 (IPv6) feature.
- TFTP IP Address—This parameter for the Cisco TFTP service no longer gets used in Cisco Unified Communications Manager Release 7.1(2). Previously, this parameter determined whether the local IP address would get used. Valid values specified True (use the local IP address) or False (use the IP address that the TFTP IP Address parameter specifies). This parameter got used in conjunction with the TFTP IP Address parameter if the TFTP server possessed multiple NICs. In that case, this parameter got set to False, and the TFTP IP Address parameter got set to the IP address of the NIC to use for serving files via TFTP.
- Server IP Track—This parameter for the Cisco TFTP service no longer gets used as of Cisco Unified Communications Manager Release 7.1(2). Previously, this parameter specified the IPv4 address of the NIC to use for serving files via TFTP. If your TFTP server possessed multiple NICs, this parameter got used in combination with the Server IP Track parameter. This parameter got set to the IP address of the NIC to use for serving files via TFTP, and the Server IP Track would get set to False. When a specific IPv4 address was set for this parameter, it had to match the value that was set in the TFTP Server 1 or TFTP Server 2 settings on the phone, or the TFTP server addresses in the DHCP options if DHCP was used for phone to obtain server addresses.

Menu Changes

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

- Main Window, page 29
- System, page 29
- Call Routing, page 30
- Media Resources, page 30
- Voice Mail, page 30
- Device, page 30
- Application, page 31
- User Management, page 31
- Bulk Administration, page 31

Main Window

The main window contains the following changes:

- After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For more information, see the "Licensing Enhancements" section on page 104.
- Customized Log-on Message—You can upload a text file that contains a customized log-on message that displays on the initial Cisco Unified Communications Manager Administration window. For more information and the procedure for uploading your customized log-on message, refer to Chapter 7 in the *Cisco Unified Communications Operating System Administration Guide*.
- Last Successful Logon—When you log in to Cisco Unified Communications Manager Administration, the initial Cisco Unified Communications Manager Administration window displays the date and time of the last successful system logon.

System

The System menu contains the following changes:

- System > Server—The IPv6 Name field displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 64.
- System > Device Pool—For new and updated incoming calling party settings, see the "Calling Party Normalization Enhancements" section on page 42. The "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50 describes the Geolocation and Geolocation Filter fields that are added in the new Geolocation Pane.
- System > Enterprise Parameters—For information on new or updated enterprise parameters, see the "New and Updated Enterprise and System Parameters" section on page 27.
- System > Service Parameters —For information on new or updated service parameters, see the "New and Updated Enterprise and System Parameters" section on page 27.
- System > LDAP > LDAP System—In the LDAP System Information field, the drop-down list box LDAP Server Type contains the new option, OpenLDAP. For this new option, the associated selections in the drop-down list box, LDAP Attribute for User ID, remain the same as for the Netscape or Sun ONE LDAP Server.

- System > Licensing > License File Upload—This window displays a message that uploading the license file removes the demo licenses for the feature. For more information, see the "Licensing Enhancements" section on page 104.
- System > Licensing > License File Upload—This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded. For more information, see the "Licensing Enhancements" section on page 104.
- System > Geolocation Configuration—This menu option allows configuration of a geolocation. For more information, see the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.
- System > Geolocation Filter—This menu option allows configuration of a geolocation filter. For more information, see the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.

Call Routing

The Call Routing menu provides the following new and updated settings.

- Call Routing > SIP Route Pattern—The IPv6 Pattern field displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 64.
- Call Routing > Directory Number—The Log Missed Calls check box displays, as described in the "Logging Missed Calls for Shared Lines" section on page 107.
- Call Routing > Logical Partitioning Policy—This window allows configuration of a logical partition policy. For more information, see the "Logical Partitioning" section on page 110.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

- Device > CTI Route Point—The Geolocation field displays, as described in the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.
- Device > Gateway—For new and updated incoming calling party settings, see the "Calling Party Normalization Enhancements" section on page 42. The Geolocation and Geolocation Filter fields display, as described in the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.
- Device > Phone—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37. The Geolocation field displays, as described in the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.
- Device > Trunk—The Destination Address IPv6 field displays for SIP trunks, as described in the "Internet Protocol Version 6 (IPv6)" section on page 64. For new and updated incoming calling party settings, see the "Calling Party Normalization Enhancements" section on page 42. In the Geolocation Configuration pane, the Geolocation and Geolocation Filter fields and the Send Geolocation Information check box display, as described in the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50.

- Device > Device Settings > Default Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.
- Device > Device Settings > Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.
- Device > Device Settings > SIP Profile—The Enable ANAT check box displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 64.
- Device > Device Settings > Common Device Configuration—The IP Addressing Mode drop-down list box, the IP Addressing Mode Preference for Signaling drop-down list box, and the Allow Auto-Configuration for Phones drop-down list box display, as described in the "Internet Protocol Version 6 (IPv6)" section on page 64.
- Device > Device Settings > Common Phone Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.

Application

No updates or new fields exist for this menu.

User Management

The User Management menu displays the following new settings:

- User Management > Role—The Find and List Roles window displays the Standard Audit Log Administration role, as described in the "Standard Audit Log Administration Role" section on page 131.
- User Management > User Group—The Find and List User Groups window displays the Standard Audit Users user group, as described in the "Standard Audit Users User Group" section on page 133.

Bulk Administration

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

- Bulk Administration > Phones > Phone Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.
- Bulk Administration > User Device Profile > UDP Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.
- Bulk Administration > Phones > Update Phones—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 37.
- Bulk Administration > Phones > Phone Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays as described in the "Logging Missed Calls for Shared Lines" section on page 107.

- Bulk Administration > User Device Profile > UDP Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays as described in the "Logging Missed Calls for Shared Lines" section on page 107.
- Bulk Administration > Phones > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls for Shared Lines" section on page 107.
- Bulk Administration > User device Profiles > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls for Shared Lines" section on page 107.
- Bulk Administration > Phones > Phone Template. Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 125.
- Bulk Administration > User Device Profile > UDP Template. Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 125.
- Bulk Administration > Gateways > Gateway Template. Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 125.
- Bulk Administration > Gateways > Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box as described in the "Support for VG202 and VG204 Gateways" section on page 150.
- Bulk Administration > Gateways > Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box as described in the "Support for VG202 and VG204 Gateways" section on page 150.
- Bulk Administration > Gateways > Insert Gateways—Select Gateway type and click Next. The second Insert Gateways Configuration window displays—Sample insert gateways link now displays VG202 and VG204 sample files along with other BAT-supported gateways as described in the "Support for VG202 and VG204 Gateways" section on page 150.
- Bulk Administration > Phone Migration—The Phone Migration window displays, as described in the "Phone Migration in BAT" section on page 150.
- Bulk Administration > Phones > Phone Template—The GeoLocation drop-down list box displays, as described in the "Support for Geolocations and Logical Partitioning" section on page 152.
- Bulk Administration > Gateways > Gateway Templates. Phone Template Configuration window—The GeoLocation drop-down list box displays, as described in the "Support for Geolocations and Logical Partitioning" section on page 152.
- Bulk Administration > Import/Export > Export—The "New fields That Are Supported for Export by Import/Export" section on page 152 describes the new fields that are supported for export by the Import/Export tool.
- Bulk Administration > Phones > Update Phones—The Apply Config button displays, as described in the "Support for Seamless Integration (Apply Config)" section on page 152.
- Bulk Administration > Phones > Reset/Restart Phones—The Apply Config button displays, as described in the "Support for Seamless Integration (Apply Config)" section on page 152.

Cisco Unified Communications Manager Features and Applications

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

- Always Use Prime Line, page 33
- Always Use Prime Line for Voice Message, page 37
- Barge, cBarge, and Single Button Barge Support for PLAR, page 39
- Calling Party Normalization Enhancements, page 42
- Cisco Unified Communications Manager Assistant Enhancements for Numeric User ID Login, page 47
- Cisco Unified Communications Manager Attendant Console Support in 7.1(2), page 48
- Cisco Web Dialer Configured in Application Server Window, page 49
- G.Clear Codec Support on SIP Trunks, page 50
- Geolocations, Geolocation Filters, and Location Conveyance, page 50
- H.235—Pass-Through Support, page 60
- H.329—Extended Video Channel Support, page 60
- Internet Protocol Version 6 (IPv6), page 64
- Licensing Enhancements, page 104
- Logging Missed Calls for Shared Lines, page 107
- Logical Partitioning, page 110
- Multicast Music On Hold Over H.323 Intercluster Trunks, page 120
- Off-Hook Abbreviated Dial, page 122
- OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database, page 125
- Party Entrance Tone, page 125
- Phone Migration in Cisco Unified Communications Manager Administration, page 128
- QSIG Variant Configuration for a Gateway or Trunk, page 130
- Synchronization of Configuration Settings, page 133
- Standard Audit Log Administration Role, page 131
- Standard Audit Users User Group, page 133
- Table Out of Sync Detection, page 136
- Unconfigured Device Registration Attempts Restricted, page 138
- Viewing Held Calls on Shared Lines, page 140

Always Use Prime Line

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

After you configure the Always Use Prime Line setting in Cisco Unified Communications Manager Administration, when the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call.

Tip To configure the Always Use Prime Line feature in previous releases of Cisco Unified Communications Manager [except for 6.1(3)], you configured the Always Use Prime Line service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(2) and 6.1(3) (or later), you can configure the Always Use Prime Line setting for devices and device profiles.

Cisco Unified Communications Manager Administration Configuration Tips

When you configure this feature, going off hook makes only the first line active, even when a call rings on another line on the phone; that is, the call does not get answered on that line. In this case, the phone user must choose the other line to answer the call.

For more configuration considerations, see Table 3 on page 34.

GUI Changes

The Always Use Prime Line setting displays in the following windows in Cisco Unified Communications Manager Administration.

- System > Service Parameters (for Cisco CallManager service)
- Device > Phone
- Device > Common Phone Profile
- Device > Device Settings > Default Device Profile
- Device > Device Settings > Device Profile

For information on how the Always Use Prime Line setting works when a phone idle or busy, see Table 3 on page 34.

Tip If you configure the Always Use Prime Line setting in the Service Parameter, Common Phone Profile, and the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

Table 3 Always Use Prime Line Configuration

State of Phone	Configuration for Always Use Prime Line	How Feature Works
Idle	On	When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. If you choose On for the Always Use Prime Line setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after the user logs in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received; that is, when the phone is off hook.

Table 3 Always Use Prime Line Configuration (continued)

State of Phone	Configuration for Always Use Prime Line	How Feature Works
Idle	Default	If you choose Default for the Always Use Prime Line setting in the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration window, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when it determines whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	When the phone already has a call on a line, Cisco Unified Communications Manager uses the configuration for the Maximum Number of Calls and Busy Trigger settings to determine how to route the call.
Idle	On, but you also configured Auto Answer With Headset or Auto Answer with Speakerphone	If you choose the Auto Answer with Headset option or Auto Answer with Speakerphone option from the Auto Answer drop-down list box in Cisco Unified Communications Manager Administration, the Auto Answer configuration overrides the configuration for the Always Use Prime Line setting.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Always Use Prime Line, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Always Use Prime Line drop-down list box, choose **True**.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(2), you can configure this feature per device or per device profile.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so activate the service by choosing **Tools > Service Activation** in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that is used by the device; for example, alwaysPrimeLine=1, which indicates that the device uses On for the configuration.

BAT Considerations

The Bulk Administration GUI includes the following updates to support the Always Use Prime Line feature: Always Use Prime Line drop-down list box—choose one of the following options:

- Off
- On

- Default

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 3.

Note The Always Use Prime Line drop-down list box displays in the Phone Template, UDP Template, and Update Phone windows.

- Insert, Export, and Validate Details support for always use prime line—The following insert, export, and validate details features receive support for the always use prime line feature:
  - 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
- UDP File Format—UDP File Format Configuration window lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Device Fields section.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "Always Use Prime Line" section on page 183.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 188.

For More Information

- Always Use Prime Line for Voice Message, page 37
- Line Select, page 188

Always Use Prime Line for Voice Message

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

After you configure the Always Use Prime Line for Voice Message setting in Cisco Unified Communications Manager Administration, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.

Tip To configure the Always Use Prime Line for Voice Message feature in previous releases of Cisco Unified Communications Manager [except for 6.1(3)], you configured the Always Use Prime Line service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(2) and 6.1(3) (or later), you can configure the Always Use Prime Line for Voice Message setting for devices and device profiles.

Cisco Unified Communications Manager Administration Configuration Tips

For configuration considerations, see Table 4 on page 38.

GUI Changes

The Always Use Prime Line for Voice Message setting displays in the following windows in Cisco Unified Communications Manager Administration.

- System > Service Parameters (for Cisco CallManager service)
- Device > Phone
- Device > Common Phone Profile
- Device > Device Settings > Default Device Profile
- Device > Device Settings > Device Profile

For information on how the Always Use Prime Line for Voice Message setting works when a phone is idle or busy, see Table 4 on page 38.

Tip If you configure the Always Use Prime Line for Voice Message setting in the Service Parameter, Common Phone Profile, and in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

Table 4 Always Use Prime Line for Voice Mail Configuration

State of Phone	Configuration for Always Use Prime Line for Voice Message	How Feature Works
Idle	On	If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. If you choose On for the Always Use Prime Line for Voice Mail setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. It will always select the first line that has a VM. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.
Idle	Default	If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration, the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration window, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when it determines whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	If the device is busy, this feature does not work.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Always Use Prime Line for Voice Message, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Always Use Prime Line for Voice Message drop-down list box, choose **True**.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(2), you can configure this feature per device.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so activate the service by choosing **Tools > Service Activation** in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that is used by the device; for example, alwaysUsePrimeLineForVM=2, which indicates that the device uses the default.

BAT Considerations

The Bulk Administration GUI includes the following updates to support the Always Use Prime Line for Voice Mail feature:

Always Use Prime Line for Voice Message drop-down list box—Choose one of the following options:

- Off
- On
- Default

Note For details of configuration options for the Always Use Prime Line for Voice Mail feature, refer to Table 4.

Note The Always Use Prime Line for Voice Message drop-down list boxes display in the Phone Template, UDP Template, and Update Phone windows.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "Always Use Prime Line" section on page 183.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 188.

For More Information

- Always Use Prime Line, page 33
- Line Select, page 188

Barge, cBarge, and Single Button Barge Support for PLAR

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

Barge, cBarge, or single-button barge allow a phone user to get added to a remotely active call that is on a shared line. Private Line Automatic Ringdown (PLAR) allows the phone user to dial a preconfigured number, and only this number, from the PLAR line. In Cisco Unified Communications Manager 7.1(2), a barge, cBarge, or single-button barge initiator can barge into a call via a shared line that is configured for PLAR; that is, the initiator can barge into the call if the barge target uses the preconfigured number that is associated with the PLAR line while on the call.

In previous releases of Cisco Unified Communications Manager [except for 6.1(3)], Cisco Unified Communications Manager sent the cBarge invocation to the PLAR line before it connected the barge call. If the PLAR line was busy in previous releases, the initiator received a busy reorder tone. In Cisco Unified Communications Manager 7.1(2) and 6.1(3) [and later 6.1(x) releases], Cisco Unified Communications Manager does not send the barge invocation to the PLAR line before it connects the barge call, so the barge occurs no matter what the state of the PLAR destination is.

Cisco Unified Communications Manager Administration Configuration Tips

To make barge, cBarge, or single-button barge work with PLAR, you must configure barge, cBarge, or single-button barge as described in the "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. In addition, you must configure the PLAR destination, a directory number that is used specifically for PLAR. The following examples describe how to enable PLAR functionality for phones that are running SCCP and for phones that are running SIP.

A and A' represent shared-line devices that you configured for barge, cBarge, or single-button barge, and B1 represents the directory number for the PLAR destination. To enable PLAR functionality from A/A', which are running SIP, see the following example:

Tip Step 1 through Step 4 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Step 1 through Step 6.

Example for How to Configure PLAR

Step 1 Create a partition, for example, P1, and a calling search space, for example CSS1, so CSS1 contains P1. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Class of Control > Partition** or **Calling Search Space**.)

Step 2 Create a translation pattern, for example, TP1, that contains calling search space CSS1 and partition P1. Create a null pattern (blank pattern), but make sure that you enter the directory number for the B1 PLAR destination in the Called Party Transformation Mask field. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Translation Pattern**.)

Step 3 Assign the calling search space, CS1, to either A or A'. (In Cisco Unified Communications Manager Administration, choose **Device > Phone**.)

Step 4 Assign the P1 partition to the directory number for B1, which is the PLAR destination. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.)

Step 5 For phones that are running SIP, create a SIP dial rule. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Dial Rules > SIP Dial Rules**. Choose **7940_7960_OTHER**. Enter a name for the pattern; for example, PLAR1. Click **Save**; then, click **Add Plar.** Click **Save**.)

Step 6 For phones that are running SIP, assign the SIP dial rule configuration that you created for PLAR to the phones, which, in this example, are A and A'. (In Cisco Unified Communications Manager Administration, choose **Device > Phone**. Choose the SIP dial rule configuration from the SIP Dial Rules drop-down list box.)

GUI Changes

No new configuration settings display in Cisco Unified Communications Manager Administration for this feature.

Service Parameter and Enterprise Parameter Changes

For parameters that you configure for barge, refer to the "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide* and the "Party Entrance Tone" section on page 125.

Installation/Upgrade (Migration) Considerations

You can use this feature after you install or upgrade to Cisco Unified Communications Manager 7.1(2).

Serviceability Considerations

No special serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

By pressing the Barge, cBarge, or Single Button Barge softkey in the remote in use call state, the initiator gets added to the call with all parties, and all parties receive a barge beep tone (if configured).

For a list of phones that support this feature, see the "Barge Tone Enhancements" section on page 185.

For More Information

- "Barge and Privacy," *Cisco Unified Communications Manager Administration Guide*
- Party Entrance Tone, page 125
- Barge Tone Enhancements, page 185

Calling Party Normalization Enhancements

Description

In Cisco Unified Communications Manager 7.1(2), the names of the Incoming Calling Party settings changed in the Device Pool, Gateway, and Trunk Configuration windows, as shown in Table 5. For information on how Cisco Unified Communications Manager 7.0(x) configuration works after an upgrade to Cisco Unified Communications Manager 7.1(2), see the "Installation/Upgrade (Migration) Considerations" section on page 47.

Table 5 Field Updates for Calling Party Normalization

Fields in Cisco Unified Communications Manager 7.0(x)	Fields in Cisco Unified Communications Manager 7.1(2)
Incoming Calling Party National Number Prefix—Allows you to configure prefixes and strip digits for the calling party number of National type.	National Number • Prefix • Strip Digits • Use Device Pool CSS (new support in 7.1(2)) • Calling Search Space (new support in 7.1(2)) In Cisco Unified Communications Manager 7.1(2), you can assign incoming calling party transformation calling search spaces for various calling party number types (Subscriber, International, National, and Unknown). Configuring these calling search spaces in the device pool, for the gateway or for the trunk, allows the device to globalize the calling party number for the various calling party number types.
Incoming Calling Party International Number Prefix—Allows you to configure prefixes and strip digits for the calling party number of International type.	International Number • Prefix • Strip Digits • Use Device Pool CSS (new support in 7.1(2)) • Calling Search Space (new support in 7.1(2))
Incoming Calling Party Subscriber Number Prefix—Allows you to configure prefixes and strip digits for the calling party number of Subscriber type.	Subscriber Number • Prefix • Strip Digits • Use Device Pool CSS (new support in 7.1(2)) • Calling Search Space (new support in 7.1(2))
Incoming Calling Party Unknown Number Prefix—Allows you to configure prefixes and strip digits for the calling party number of National type.	Unknown Number • Prefix • Strip Digits • Use Device Pool CSS (new support in 7.1(2)) • Calling Search Space (new support in 7.1(2))

Cisco Unified Communications Manager Administration Configuration Tips

This section contains information on the following topics:

- Considerations for Configuring the Prefix Field, page 43
- Considerations for Configuring the Strip Digits Field, page 43

Considerations for Configuring the Prefix Field

Before you configure the prefix fields, consider the following information.

- In the Device Pool, Gateways, and Trunk Configuration windows, to delete the prefixes in all incoming calling party settings at the same time, click **Clear Prefix Settings**; to enter the default value for all incoming calling party settings at the same time, click **Default Prefix Settings**.
- If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
- To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.
- When the prefix gets applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions, such as supplementary services, including call forwarding, call park, voice messaging, CDR data, and so on, that pertain to the call.
- If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix. (For example, the calling party number arrives empty because you chose Restricted from the Calling Line ID Presentation drop-down list box in the Route Pattern, Gateway, or Trunk Configuration windows.)
- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.
- Configure the incoming prefix fields in conjunction with the strip digit fields; that is, if your service provider prepends leading digits (for example, a zero) to the calling party number. For more information on stripping leading digits from the calling party number, see the "Considerations for Configuring the Strip Digits Field" section on page 43.

Considerations for Configuring the Strip Digits Field

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the Strip Digits fields to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

Before you configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number, consider the following information.

- You can either strip digits by configuring the Incoming Prefix service parameters in the Service Parameters window or by configuring the Strip Digits fields in the Device Pool, Gateway, or Trunk Configuration windows. For information on how to configure the service parameters for this functionality, see the "Service Parameter and Enterprise Parameter Changes" section on page 45.

- If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.
- To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.
- Be aware that Cisco Unified Communications Manager can strip up to 24 digits. If you enter a value that is larger than 24 in the field, for example, 26, Cisco Unified Communications Manager Administration does not allow the configuration.
- If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix.
- If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).
- If you do not configure a value for the Strip Digits fields, Cisco Unified Communications Manager does not strip any digits from the calling party number.
- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

GUI Changes

The settings in Table 5 display in the following windows in Cisco Unified Communications Manager Administration:

- Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device.
- Gateway (Device > Gateway)—Displays settings in the H.323 gateway configuration window and in the port windows (Gateway Configuration window) for MGCP (T1-PRI/BRI) and MGCP (E1-PRI/BRI).
- Trunk (Device > Trunk)—Displays all settings in all trunk configuration windows except the SIP trunk.

Tip The SIP Trunk Configuration window only displays the Unknown Number settings.

For configuration procedures for each configuration window, refer to the following sections:

- Configuring a Device Pool, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide*

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameters changes occurred for this feature in 7.1(2).

Tip To locate the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**; choose the server and the Cisco CallManager service. After the parameters display, click **Advanced**. For information on the service parameter, click the hyperlink for the service parameter name or the question mark that displays in the upper, right corner of the window.

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can enter a colon (:) followed by the number of digits that you want to strip in the Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and/or Incoming Calling Party Subscriber Number Prefix service parameters to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. The value that you configure before the colon (:) represents the prefix; the value that you configure after the colon (:) specifies the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number before it applies the prefix.

For example, you configure +:1 in the incoming prefix service parameters, which alerts Cisco Unified Communications Manager to strip the first digit from the calling party number and then apply the international escape character +. If an incoming call arrives as 04423452345, Cisco Unified Communications Manager strips the first digit, in this case, zero, from the calling party number and prefixes the international escape character + to the calling party number. As a result, the calling party number gets transformed to +4423452345.

To strip digits without prefixing anything, you can configure the colon (:) in the incoming prefix service parameters without configuring a prefix. If you do not enter a prefix before the colon (:), Cisco Unified Communications Manager strips the number of leading digits that you specify and does not apply a prefix to the calling party number. For example, if you configure :2, Cisco Unified Communications Manager strips 2 leading digits without applying a prefix.

If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix. For example, if you enter +1:6 in the incoming prefix fields, and the calling party number contains 6 or fewer digits, Cisco Unified Communications Manager strips all digits and applies the prefix +1.

If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).

If you do not configure a colon (:) in the incoming prefix service parameters, Cisco Unified Communications Manager does not strip any digits from the calling party number; that is, unless you configure the Strip Digit fields that are listed in Table 5, which support the configuration at the device level.

If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix.

Cisco Unified Communications Manager can strip up to 24 digits from the calling party number. If you enter :26 in the incoming prefix service parameters, Cisco Unified Communications Manager Administration displays a message and does not allow the configuration.

If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Tip If you configure the incoming fields that display in the device configuration windows and the service parameters, Cisco Unified Communications Manager uses the configuration that you configured in the device configuration window.

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

Tip If you have a single H.323, MGCP (T1-PRI/BRI), or MGCP (E1-PRI/BRI) gateway in your network, you can configure the prefix service parameters, which support the Cisco CallManager service, for the particular gateway type in the Service Parameter Configuration window. If you configure the prefix service parameters for a particular gateway type, for example, H.323, be aware that all H.323 gateways that you configure in Cisco Unified Communications Manager Administration use the configuration from the service parameter unless you configure the prefix settings for a particular gateway in the Gateway Configuration window.

- Incoming Calling Party National Number Prefix - H.323
- Incoming Calling Party International Number Prefix - H.323
- Incoming Calling Party Subscriber Number Prefix - H.323
- Incoming Calling Party Unknown Number Prefix - H.323

Tip If the incoming prefix service parameters for H.323 use the same prefix as the incoming prefix service parameters for the phone, the prefix gets used twice for the calling party; first, when the incoming call gets to the gateway and again, when the call terminates at the phone.

- Incoming Calling Party Unknown Number Prefix - SIP

Installation/Upgrade (Migration) Considerations

If you upgrade from Cisco Unified Communications Manager 7.0(1) to 7.1(2), be aware that Cisco Unified Communications Manager moves the numbers of digits that you want stripped from the Incoming Prefix 7.0 fields in the Device Pool, Trunk, or Gateway Configuration windows to the Strip Digits fields in the same windows in Cisco Unified Communications Manager Administration 7.1(2). For example, if you configured :12 in the Incoming Calling Party International Number Prefix field in the Trunk Configuration window in 7.0(1), 12 displays in the Strip Digits field for the International Number in the Trunk Configuration window after you upgrade to 7.1(2).

If you configured the Incoming Prefix service parameters in 7.0(1) so Cisco Unified Communications Manager strips leading digits, Cisco Unified Communications Manager 7.1(2) does not change the configuration; that is, Cisco Unified Communications Manager 7.1(2) uses the value, including the : (colon), that you configured in 7.0(1).

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that this service is activated in Cisco Unified Serviceability.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "Enhancements to Calling Party Number Transformations" section on page 182.

User Tips

Depending on your configuration, a phone user may not need to edit the call log directory entry on the phone before placing a call. Depending on your configuration, the phone user may see the international escape character, +, in the call log directories on the phone.

For More Information

- "Calling Party Normalization" chapter, *Cisco Unified Communications Manager Features and Services Guide*

Cisco Unified Communications Manager Assistant Enhancements for Numeric User ID Login

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Cisco Unified Communications Manager supports numeric user ID login for Cisco Unified Communications Manager Assistants from their Cisco Unified IP Phones.

To configure numeric user ID login, perform the following steps:

Procedure

Step 1 When you are adding a Cisco Unified Communications Manager Assistant user (in Cisco Unified Communications Manager Administration, go to **User Management -> End User**), assign a User ID that is numeric only.

Step 2 In Cisco Unified Communications Manager Administration, go to the Service Parameters window (**System> Service Parameters**); then, select your server and select the Cisco IP Manager Assistant service.

In the section “Clusterwide Parameters (Parameters that apply to all servers)” set Alpha Numeric UserID to **False**.

Step 3 Restart the Cisco IP Manager Assistant service for this configuration change to take effect.

Cisco Unified Communications Manager Attendant Console Support in 7.1(2)

If you are upgrading from a compatible Cisco CallManager 4.X release or a compatible Cisco Unified Communications Manager 5.X, 6.X, or 7.X release to Cisco Unified Communications Manager Release 7.1(2), you can continue to use the Cisco Unified Communications Manager Attendant Console. As automated within the Cisco Unified Communications Manager upgrade process, the Cisco Unified Communications Manager Attendant Console plug-in will remain viewable from the Find and List Plugins window in Cisco Unified Communications Manager Administration 7.1(2).

Be aware, however, that Cisco no longer supports the Cisco Unified Communications Manager Attendant Console with new installations of Cisco Unified Communications Manager 7.X. For new installations, the Cisco Unified Communications Manager Attendant Console plug-in does not display in the Find and List Plugins window in Cisco Unified Communications Manager Administration.

If you previously obtained the Cisco Unified Communications Manager Attendant Console 7.0(x) plug-in from the Cisco software download site, you can use that plug-in with Cisco Unified Communications Manager 7.1(x) but only for upgrades of a compatible Cisco Unified Communications Manager 5.X, 6.X, or 7.X release to Cisco Unified Communications Manager Release 7.1(x). Cisco Systems does not authorize the use of the Cisco Unified Communications Manager Attendant Console 7.0(x) plug-in with new Cisco Unified Communications Manager 7.X installations, and its use does not get supported by the Cisco Technical Assistance Center.

If you need attendant console functionality after a Cisco Unified Communications Manager 7.X installation/upgrade, Cisco recommends that you use the Cisco Unified Business Attendant Console, Cisco Unified Enterprise Attendant Console, or the Cisco Unified Department Attendant Console.

For More Information

- Cisco Unified Communications Manager Attendant Console End of Life and End of Sale Announcement—http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7046/ps7282/end_of_life_notice_c51-499091.html
- *Cisco Unified Communications Manager Software Compatibility Matrix* —For information on the versions of Cisco Unified Business Attendant Console, Cisco Unified Enterprise Attendant Console, or Cisco Unified Department Attendant Console that are compatible with Cisco Unified Communications Manager 7.1(2)
- http://www.cisco.com/en/US/products/ps7282/tsd_products_support_series_home.html

  To obtain the documentation for Cisco Unified Business Attendant Console, Cisco Unified Enterprise Attendant Console, or Cisco Unified Department Attendant Console, click the **Release Notes** link or the **Maintain and Operate** link after you go to the preceding URL.
- “Cisco Unified Communications Manager Attendant Console” chapter, *Cisco Unified Communications Manager Features and Services Guide*

Cisco Web Dialer Configured in Application Server Window

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

In previous releases of Cisco Unified Communications Manager [except for 6.1(3)], the List of WebDialers field in the Service Parameter window supported a maximum of 255 characters, which limited the scalability of the Redirector. In Cisco Unified Communications Manager 7.1(2) and 6.1(3), you configure the WebDialer servers in the Application Server Configuration window instead of the Service Parameters Configuration window.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

You can add a Cisco Web Dialer application server through the Application Server Configuration window. You access the Application Server Configuration window by choosing **System > Application Server** in Cisco Unified Communications Manager Administration. Cisco Web Dialer displays as one of the options in the Application Server Type drop-down list box.

If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of Web Dialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service.

Service Parameter and Enterprise Parameter Changes

In Cisco Unified Communications Manager 7.1(2), you can configure either the List of WebDialers service parameter or the Cisco Web Dialer application server through the Application Server Configuration window. If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service. You can access the Service Parameter Configuration window by choosing **System > Service Parameters** in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

If you install Cisco Unified Communications Manager 7.1(2) and plan to use Cisco Web Dialer, configure the Cisco Web Dialer application server in the Application Server Configuration window. You do not need to configure the List of WebDialers field in the Service Parameter Configuration window if you configure the application server in the Application Server Configuration window.

Serviceability Considerations

Cisco Web Dialer relies on the Cisco WebDialer Web Service. If you have not already done so, activate this service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

User Tips

For user enhancements for Cisco Web Dialer, see the "Cisco Web Dialer Enhancements" section on page 192.

For More Information

- "Cisco Web Dialer" chapter, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Web Dialer Enhancements, page 192

G.Clear Codec Support on SIP Trunks

Cisco Unified Communications Manager supports limited early offer for G.Clear data calls (also known as clear channel). The Early Offer for G.Clear Calls feature provides support for third-party SIP user agents that can do early offer to negotiate data calls without using a Media Termination Point. MTPs do not support the G.Clear codec.

If you enable both Media Termination Point Required and Early Offer for G.Clear Calls for a SIP device, the system does not allocate the MTP if the G.Clear codec in present in the offer. The system only allocates the MTP if the call is not G.Clear, and the MTP is required.

The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP), including CCD, G.nX64, and X-CCD.

To enable or disable Early Offer for G.Clear Calls, navigate to the SIP Profile Configuration window in Cisco Unified Communications Manager Administration (**Device Device Settings > SIP Profile**) and choose one of the following options for the **Early Offer for G.Clear Calls** parameter:

- Disabled (default)
- CLEARMODE
- CCD
- G.nX64
- X-CCD

AXL and CTI Considerations

See the "Enhanced Clear Channel (G.clear) Support" section on page 182.

Geolocations, Geolocation Filters, and Location Conveyance

This section, which describes geolocations, geolocation filters, and location conveyance for Cisco Unified Communications Manager 7.1(2), contains information on the following topics:

- Description for Geolocations, page 51
  - Geolocation Usage for Shared Lines and Route Lists, page 53
  - Geolocation Examples, page 53
  - Geolocation Identifiers, page 53
- Description for Geolocation Filters, page 54
  - Geolocation Filter Examples, page 54
- Description for Location Conveyance, page 55
- Interactions for Location Conveyance, page 55
- Geolocation Configuration Tips, page 55

- Geolocation Filter Configuration Tips, page 56
- Location Conveyance Configuration Tips, page 57
- GUI Changes for Geolocations and Geolocation Filters, page 58
- Service Parameter and Enterprise Parameter Changes for Geolocations and Geolocation Filters, page 58
- Installation/Upgrade (Migration) Considerations for Geolocations and Geolocation Filters, page 59
- Serviceability and RTMT Considerations, page 59
- BAT Considerations, page 59
- CAR/CDR Considerations, page 59
- Security Considerations, page 59
- For More Information, page 60

Description for Geolocations

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.

Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.

The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC.

In Cisco Unified Communications Manager Administration, geolocations get configured manually.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System > Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System > Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Configuration of geolocations entails provisioning the following elements:

- Configure geolocation identifiers
  - You can define sets of geolocations (civic addresses).
  - You can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
  - You can define geolocation filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.

Cisco Unified Communications Manager administrators must define the following item:

- A *geolocation* for every device that participates in any feature that requires geolocations. The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC. Geolocations get configured manually.

Cisco Unified Communications Manager administrators then assign geolocations to devices.

The following entities in a Cisco Unified Communications Manager cluster can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports

Note Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

You do not need to associate media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, with geolocations.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The intercluster trunk (ICT) or SIP trunk device layer that receives this information uses the information for location conveyance.
4. No communication of geolocation from Cisco Unified Communications Manager to a phone takes place.

The following logic determines the geolocation value:

1. Read the value for geolocation from the device window. If it is not configured in the device window, for phone device in roaming, read the device pool (DP) from the roaming configuration. For phone device that is not in roaming, read the DP from the device configuration.
2. For trunk, ICT, or MGCP port device, read the DP from the device configuration.
3. From the selected DP, read the value of geolocation from DP configuration window.
4. If DP is not configured with a value for Geolocation, use blank value.
5. If available geolocation value is blank, call processing uses the configured value that the Default Geolocation enterprise parameter specifies.

The standard record for a geolocation specifies *Unspecified*. Use this value when no geolocation needs to associate with a device. In such scenarios, any features that are based on geolocations do not execute. Also, devices for which no geolocation gets specified do not participate in geolocation information conveyance across clusters for intercluster calls.

Be aware that the Default Geolocation enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, you do not know the actual connected device until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- When a device answers, the actual geolocation information for the device becomes available and gets communicated to call control and to any features that are involved.

Geolocation Examples

Table 6 specifies examples of geolocations.

Table 6 Geolocation Examples

Geolocation Name	Geolocation Data
IN-KA-BLR-BLD1	(country=IN, A1=KA, A3=Bangalore, A4= A4, A5=12, A6=Langford Road, PRD=12, LOC=BLD1, NAM=unified comm, PC=560001)
IN-KA-BLR-BLD2	(country=IN, A1=KA, A3=Bangalore, A4= A4, A6=Outer Ring Road, LOC=BLD2, NAM=unified comm, PC=560002)
IN-MH-MUM-BLD1	(country=IN, A1=MH, A3=Mumbai, A4= A4, LOC=bld1, NAM=unified comm, PC=220001)
IN-KA-BLR-ICTtoSJ	(country=IN, A1=KA, A3=Bangalore, NAM=ICTToSJ)

Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

Geolocation filters allow selection of specific fields from the 17 geolocation fields. Use the **System > Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters manually. Specific Cisco Unified Communications Manager features associate the geolocation filters by using drop-down list boxes in the configuration windows of the devices that get configured for a particular feature.

The Cisco Unified Communications Manager device type of a device specifies one of the following values:

- Border—Use this value to specify accessing PSTN trunks, intercluster trunks (ICTs), gateways, and MGCP ports.
- Interior—Use this value for VoIP phones or internal endpoints.

Refer to Table 21 in the “Logical Partitioning” section for a detailed listing of the Cisco Unified Communications Manager devices that associate with the Border and Interior device types.

The following object specifies an example geolocation identifier:

> {**geolocPkid**=9dc76052-3a37-78c2-639a-1c02e8f5d3a2, **filterPkid**=d5bdda76-6a86-56c5-b5fd-6dff82b37493, **geolocVal=**, devType=8}

where:

The geolocVal field gets used in cases where the Cisco Unified Communications Manager database does not reference the geolocation record but data for a geolocation comes from another source (for example, location conveyance PIDF-LO XML from a remote cluster).

In such cases, Cisco Unified Communications Manager constructs the name value pair for the geolocation fields.

Example: "country=US:A1=Texas:A3=Richardson:LOC=Building 6" where the value gets communicated through the geolocVal field.

Note In such a case, the geolocPkid gets kept null, and call control or features access the geolocVal field from a geolocation identifier.

The following string specifies the logical representation of a geolocation identifier:

"Border:country=US:A1=Texas:A3=Richardson:LOC=Building 6"

Note This geolocation identifier gets constructed from the member fields of a geolocation identifier.

Description for Geolocation Filters

Cisco Unified Communications Manager administrators define the following item:

- A *geolocation filter* for every device that participates in a feature that uses geolocation filters. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

The following logic determines the geolocation filter value:

1. For phone device that is in roaming, read the geolocation filter value from DP in roaming configuration. For phone device that is not in roaming, read the geolocation filter value from DP in device configuration.
2. For trunk, intercluster trunk, or MGCP port device, read geolocation filter value from device window. If no value is configured, read from DP.
3. If DP is not configured with a geolocation filter value, use blank value.
4. If available filter is blank, call processing uses the value that the Default Geolocation Filter enterprise parameter specifies.

Geolocation Filter Examples

Table 7 specifies examples of geolocation filters.

Table 7 Geolocation Filter Examples

Geolocation Name	Geolocation Filter Data
India-Filter1	(UseCountry, UseA1, UseA3, UseLOC)
India-GW-Filter2	(UseCountry, UseA1, UseA3, UseLOC, UseNAM)
India-ICT-Trunk-Filter3	(UseCountry, UseA1, UseA3, UseNAM)

Description for Location Conveyance

Location conveyance involves configuration to make the following behavior possible:

- Communicate geolocation information across clusters
  - Allow communication of geolocation information from one cluster to another, at call establishment as well as midcall joins and redirects.

Note Enterprise parameters and logical partitioning configuration do not control location conveyance. If a device that communicates through a trunk associates with geolocation information, check the Send Geolocation Information check box when you configure the trunk (either SIP or ICT) to convey the geolocation information across clusters.

For the logical partitioning feature, the Cisco Unified Communications Manager does not send the configured geolocation information to line devices (phones that are running SIP or SCCP).

Interactions for Location Conveyance

The location conveyance feature interacts as follows:

- Geolocation conveyance across SIP trunks and intercluster trunks
- SIP trunk error handling for geolocation information
- Intercluster trunk error handling for geolocation information
- Handling a received geolocation
- Feature interactions with midcall geolocation change

Geolocation Configuration Tips

Use the **System > Geolocation Configuration** menu option in Cisco Unified Communications Manager Administration to configure geolocations.

Table 8 provides a checklist for configuring geolocations.

Table 8 Geolocation Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Define a set of geolocations on a new Geolocation Configuration window.	Geolocation Configuration
Step 2	Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*

Table 8 Geolocation Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.	Geolocation Configuration Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 4	For devices that do not participate in features that require geolocations, define the geolocation as *Unspecified* or leave undefined. **Note** You can define this lack of association at the individual-device level, the device-pool level, or the enterprise-parameter level.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*

Geolocation Filter Configuration Tips

Use the **System > Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

Table 9 provides a checklist for configuring geolocation filters.

Table 9 Geolocation Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Define a set of filter rules in a new Geolocation Filter Configuration window.	Geolocation Filter Configuration
Step 2	Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 3	For the logical partitioning feature, assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning

Location Conveyance Configuration Tips

Table 10 provides a checklist for configuring location conveyance in a multicluster logical partitioning environment.

Table 10 Location Conveyance Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Define a set of geolocations in a new Geolocation Configuration window.	Geolocation Configuration
Step 2	Assign geolocations to device pools, devices, SIP trunks, intercluster trunks, gateways, or MGCP ports for the devices that need to participate in location conveyance.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*

Table 10 Location Conveyance Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 3	Assign geolocations to a default geolocation that the Default Geolocation enterprise parameter specifies. This assignment allows you to specify a default geolocation for a cluster. For devices for which no associated geolocation exists at the device or device-pool level, the value that is specified by the Default Geolocation enterprise parameter applies.	Geolocation Configuration Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 4	If geolocation information about devices needs to be communicated across clusters, ensure that location conveyance is configured. To do so, check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk for the devices that need to pass geolocation information across clusters as follows: • Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster. • Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.	Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*

GUI Changes for Geolocations and Geolocation Filters

Use the following new menu options in Cisco Unified Communications Manager Administration to configure the geolocations and geolocation filters:

- System > Geolocation Configuration
- System > Geolocation Filter

The following existing Cisco Unified Communications Manager Administration windows contain new fields for configuring geolocations and geolocation filters:

- Device Pool Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter
- CTI Route Point Configuration—field: Geolocation
- Gateway Configuration—pane: Geolocation Configuration; fields: Geolocation, Geolocation Filter
- Cisco Unified IP Phone Configuration— field: Geolocation
- Trunk Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter, Send Geolocation Information

Service Parameter and Enterprise Parameter Changes for Geolocations and Geolocation Filters

The following new enterprise parameter affects the configuration of geolocations:

- Default Geolocation

Installation/Upgrade (Migration) Considerations for Geolocations and Geolocation Filters

The following migration considerations that affect the dial plan exist for geolocations and geolocation filters when you are migrating from releases of Cisco Unified Communications Manager that are earlier than Release 7.1(2):

- If the Enable Logical Partitioning enterprise parameter is set to **True**, ensure geolocations and geolocation filters are configured for the following entities:
  - Device pools for all phones
  - MGCP ports that access the PSTN
  - H.323 gateways that access the PSTN
  - Intercluster trunks (ICTs, either gatekeeper-controlled or non-gatekeeper-controlled) to remote clusters
  - SIP trunks that access the PSTN or remote clusters
- Ensure that location conveyance is turned on in all clusters to allow end-to-end communication of geolocation information.

  To do so, check the Send Geolocation check box on intercluster trunks (ICTs) and SIP trunks.

During upgrade of Cisco Unified Communications Manager Release 7.1(x) or later from an earlier release, the following values get assigned for the entities that associate with configuration of geolocations and geolocation filters:

- Geolocation
  - No configured geolocation records exists in the geolocation table.
  - Default Geolocation enterprise parameter specifies **Unspecified**.
  - Device pools specify Geolocation value **None**.
  - Devices specify Geolocation value **Default**.
- Geolocation filter
  - No configured geolocation filter records exist in geolocation filter table.
  - Logical Partitioning Default Filter enterprise parameter specifies **None**.
  - Device pools specify Geolocation Filter value **None**.
  - Devices specify Geolocation Filter value **None**.

Serviceability and RTMT Considerations

No serviceability nor RTMT considerations exist for geolocations, geolocation filters, or location conveyance.

BAT Considerations

The Cisco Bulk Administration Tool specifies several new menu items to support geolocations. See the "Support for Geolocations and Logical Partitioning" section on page 152 for details.

CAR/CDR Considerations

No CAR/CDR considerations exist for geolocations, geolocation filters, or location conveyance.

Security Considerations

No security considerations exist for geolocations, geolocation filters, or location conveyance.

For More Information

- Geolocations and Location Conveyance, *Cisco Unified Communications Manager Features and Services Guide*
- Logical Partitioning, *Cisco Unified Communications Manager Features and Services Guide*
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*
- Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
- CTI Route Point Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Call Detail Records Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Reporting Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Assistant User Guide*

H.235—Pass-Through Support

Consider the following:

During a call that employs H.235 encryption, do not invoke mid-call features such as call transfer or hold/resume operations. If you do, the call may become unencrypted.

Cisco Unified Communications Manager does not support H.235 encryption when a media termination point or transcoder gets inserted into a call. If this occurs, the call will become unencrypted.

H.329—Extended Video Channel Support

The extended video channels feature works via H.239 protocol and enables multiple video channel support. Cisco Unified Communications Manager supports negotiating an extended video channel by using the H.239 protocol in direct point-to-point H.323 calls. This also includes calls across the H.323 intercluster trunk.

Cisco Unified Communications Manager supports all H.239 associated support signals and commands that are specified in the H.239 recommendation.

The following characteristics apply to the extended video channels feature:

- Support for Third-Party H.323 Devices, page 61

- H.323 Devices Invoke Presentation Feature, page 61
- Opening Second Video Channels, page 62
- Call Admission Control (CAC) on Second Video Channels, page 63
- Number of Video Channels Allowed, page 63
- H.239 Commands and Indication Messages, page 63
- Topology and Protocol Interoperability Limitation, page 64
- Mid-Call feature Limitation, page 64

Support for Third-Party H.323 Devices

The extended video channel feature supports H.239 interoperability among third-party video endpoints and Cisco Unified Voice Conferencing. Cisco Unified Communications Manager allows an extended video channel to be used for presentation and live meeting transmission. This feature focuses on multiple video channel support via H.245 signaling. The following presentation applications provide basis for this multichannel support:

- Natural Presenter package by the third-party vendor Tandberg
- People + Content by the third-party vendor Polycom

Both Natural Presenter package and People + Content use the H.239 protocol to negotiate capabilities and define the roles of the additional video channels.

Note Natural Presenter package by Tandberg and People + Content by Polycom only support H.239 for the presentation mode.

Note Be aware that the presentation applications that are offered by Tandberg and Polycom are optional features. You must have one of these options and H.239 enabled in both caller and callee endpoints to negotiate second video channels, or the call will get limited to a single video channel.

H.323 Devices Invoke Presentation Feature

Tandberg and Polycom terminals allow the user to share presentation materials from various components (for example, VCR, Projector, PC, and so on). The components can physically connect with the terminals, and the PC can also run presentation applications that are provided by the vendor to transmit the presentation image. Be aware that the source of presentation and the component connection with the terminal are irrelevant to the mechanism of establishing video channels by using H.239.

Note For details on setting up presentation sources, refer to the video terminal user guide.

When two H.239-enabled terminals attempt to establish a video call, they declare their video capabilities for the main video channel for meeting participants and their extended video capabilities (H.239 capabilities) for the second video channel. The following contents comprise H.239 capability signals:

1. The terminals send signals to indicate that the devices support H.239. They also send associated commands and indication signals for managing the second video channel. This enables both the terminals to be aware that the call is capable of opening multiple video channels.

2. The terminal sends out one or more extended video codec capabilities to express video codec capabilities for second channels. The terminal must specify the role of the second video channel. The defined role labels can be
   - Live-video—This channel gets processed normally and is suitable for live video of people.
   - Presentation—This channel relays a token-managed presentation that is distributed to the devices.

After the capabilities have been exchanged, both terminals immediately open two-way audio channels and the main video channels as in the traditional video calls.

Opening Second Video Channels

Depending on the third-party terminal implementation, the second video channel gets handled differently among vendors.

Natural Presenter Package by Tandberg

Tandberg initiates the second video channel on demand. A Tandberg device does not open the second video channel immediately after the main video channel is established. The second channel gets opened when one of the callers (the presenter) specifies the source of the presentation and invokes a command to start the presentation.

When a Tandberg user decides to start sharing the presentation, Tandberg requests the other call party to open an extended video channel for receiving the presentation image; therefore, a Tandberg-Tandberg call has only one-way second video channel.

People + Content by Polycom

Unlike Tandberg, a Polycom terminal initiates the second video channel immediately as a part of the default mechanism, after both parties have confirmed that additional video channels can get supported.

Note The channel gets established automatically if both parties support H.239 and have the extended video channel feature enabled; however, the additional channel does not show anything until one of the parties starts to share presentation.

Polycom initiates a request for the second video channel to the other call party regardless of the usage of the second video channel; therefore, in a Polycom-Polycom call, two-way video channels get opened between the devices even if only one of them sends out presentation image/video.

This implementation ensures that both call parties have the second video channel ready for transmission when the call parties decide to take the token to present something. Although one of the two video channels remains idle (not sending anything), the Polycom device controls bandwidth to ensure load efficiency.

Note This difference in handling second video channels does not affect the implementation of H.239. Cisco Unified Communications Manager does not initiate any receiving channel request in an H.323-H.323 call. Cisco Unified Communications Manager simply relays all channel requests from one terminal to another.

Note Cisco Unified Communications Manager does not enforce two-way transmission for the second set of video channels because this does not represent a requirement in the H.239 protocol.

Call Admission Control (CAC) on Second Video Channels

The following call admission control policies of Cisco Unified Communications Manager get applied to the second video channels:

Cisco Unified Communications Manager restricts the bandwidth usage by the second video channels on the basis of location configuration. When the second video channel is being established, Cisco Unified Communications Manager makes sure that enough video bandwidth stays available within the location pool and reserves bandwidth accordingly. If the required bandwidth is not available, Cisco Unified Communications Manager instructs the channel to reduce the available bandwidth to zero.

No change occurs in the region configuration or policies to support the second video channels.

Traditionally, Cisco Unified Communications Manager region policy only supported a call with a single video channel, and the total bandwidth usage of this call never gets larger than what the region configuration specifies.

If the administrator sets a finite region video bandwidth restriction for an H.239 call, Cisco Unified Communications Manager will violate the region policy because the region value will get used against the bandwidth that is requested for each video channel independently.

Example:

```
If the region video bandwidth is set to 384Kbps and the audio channel uses 64Kb/s, the
maximum allowed bandwidth for each video channel will be (384Kb/s - 64Kb/s)= 320Kb/s.
i.e. the maximum bandwidth to be used by the H.239 call will be (audio bw + 2*(384 - audio
bw)) = 704Kb/s, which goes beyond the 384Kb/s bandwidth that the region specifies.
```

Note You should consider relaxing both region and location bandwidth restrictions for H.239 calls, so the H.239 devices are allowed to readjust and balance load for both the video channels without Cisco Unified Communications Manager intervention.

Number of Video Channels Allowed

Cisco Unified Communications Manager 7.1(2) supports only a maximum of two video channels due to the following reasons:

- Both Tandberg and Polycom only support two video channels, one of which is for main video, and the other is for presentation.
- H.239 only defines an Additional Media Channel (AMC) for H.320-based system to partition the traditional H.320 video channel for the purpose of presentation.

H.239 Commands and Indication Messages

Command and Indication (C&I) messages get used for H.239 to manage tokens for the Presentation and Live roles and to permit devices to request release of video flow control to enable the operation of additional media channels. Cisco Unified Communications Manager supports all the C & I messages. Whenever Cisco Unified Communications Manager receives C&I messages, it relays them to the call party accordingly.

Be aware that the flow control release request and response messages can be used to request that the far end release flow control, so it allows an endpoint to send the indicated channel at the indicated bit rate.

Note Be aware that the call party may or may not honor the request as is indicated by flow control release response.

The Presentation role token messages allow an H.239 device to acquire the token for presentation. The other call party may accept or reject the request. The presenter device sends out a token release message when it is no longer needed.

Topology and Protocol Interoperability Limitation

Cisco Unified Communications Manager 7.1(2) supports only H.239 in H.323 to H.323 calls. Cisco Unified Communications Manager allows H.239 calls to be established across H.323 intercluster trunk or multiple nodes. If an H.239-enabled device attempts to make a call with a non-H323 end, the H.239 capabilities will get ignore, and the call will get conducted like the traditional video calls that supported Cisco Unified Communications Manager supports.

Cisco Unified Communications Manager does not support a second video channel when a media termination point or transcoder is inserted into the call. If it happens, the call will fall back to normal video calls.

Mid-Call feature Limitation

Cisco Unified Communications Manager supports opening second video channels only in direct H.323 to H.323 calls.

Caution Do not attempt to invoke any mid-call features such as call transfer or hold/resume operations. Doing so can lead to problems, and the second video channel can get disconnected.

Internet Protocol Version 6 (IPv6)

This section, which describes IPv6 support for Cisco Unified Communications Manager 7.1(2), contains information on the following topics:

- Description for IPv6 Support, page 64
- Interactions and Restrictions for IPv6, page 65
- IPv6 Configuration Tips, page 68
- Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 70
- Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 73
- Service Parameter and Enterprise Parameter Changes for IPv6, page 78
- Installation/Upgrade (Migration) Considerations for IPv6, page 79
- Serviceability and RTMT Considerations for IPv6, page 80
- CAR/CDR Considerations for IPv6, page 83
- Security Considerations for IPv6, page 84
- Supported Phone Models for IPv6, page 85
- Phone Considerations, page 85
- For More Information, page 103

Description for IPv6 Support

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications

Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* contains descriptive information on the following topics:

- Cisco Unified Communications Manager and IPv6
- Cisco Unified IP Phones and IPv6
- DHCPv6 and IPv6
- DNS and IPv6
- Gateways and IPv6
- Media Termination Points and IPv6
- SIP Trunks and IPv6
- TFTP Server and IPv6

Tip Before you configure IPv6, review the "Internet Protocol Version 6 (IPv6)" chapter carefully. For example, this chapter describes how to configure the Cisco Unified Communications Manager server and phones in dual-stack mode. It also describes how Cisco Unified Communications Manager uses MTPs to translate IPv4 to IPv6 (or vice versa) and so on.

Interactions and Restrictions for IPv6

Some Cisco Unified Communications Manager features do not work for devices with an IP Addressing Mode of IPv6 Only. Before you configure IPv6 Only for a device, review the following section, which describes Cisco Unified Communications Manager feature interactions and restrictions for IPv6.

- Annunciator—Annunciator supports IPv4; if annunciator connects to a device with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6. If no MTP that can translate IP address versions is available, no announcement plays on the phone.
- Call Detail Records—See the "CAR/CDR Considerations for IPv6" section on page 83.
- Cisco Certificate Authority Proxy Function—See the "Security Considerations for IPv6" section on page 84.
- Cisco Extension Mobility—Cisco Extension Mobility supports IPv4, so you cannot use phones with an IP Addressing Mode of IPv6 Only for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.
- Cisco Unified Communications Operating System—See the "Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window" section on page 70.
- Cisco Unified Serviceability— See the "Serviceability and RTMT Considerations for IPv6" section on page 80.
- Cisco Unity Connection and Cisco Unity—Cisco Unity Connection and Cisco Unity communicate with Cisco Unified Communications Manager by using IPv4.

- Cisco Unified Communications Manager Assistant—Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.
- Cisco Unified Real-Time Monitoring Tool—See the "Serviceability and RTMT Considerations for IPv6" section on page 80.
- Cisco Web Dialer—Cisco Web Dialer supports IPv4, so, to connect to CTI Manager, Cisco Web Dialer uses an IPv4 address. Cisco Web Dialer works with devices with an IP Addressing Mode of IPv4 and IPv6.
- Conferences—Cisco Unified Communications Manager uses IPv4 for conferences, even if the conference bridge uses IPv6. During a conference, Cisco Unified Communications Manager inserts one MTP that can translate IPv4 to IPv6 for each device with an IP Addressing Mode of IPv6 Only, so each phone that uses an IPv6 address can join the conference.

  For your MTP device to support security, you must configure the MTP in passthru mode, which means that the MTP does not transform the packets during the call. When you configure an MTP in passthru mode, the MTP gets the encrypted packet on one call leg and sends out the same packet on a different leg of the call. For secure conferences with secure conference bridges and encrypted devices with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP into the conference to translate IPv4 to IPv6 (and vice versa) when some devices in the conference support IPv4. If you configure the MTP for passthru mode, the encrypted IPv6 phones communicate with the conference bridge via SRTP. If you do not configure the MTP for passthru mode, the media gets downgraded to RTP.
- Device Mobility—Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility.
- Differentiated Services Control Point (DSCP)—Be aware that Differentiated Services Control Point (DSCP) values are the same for both IPv6 and IPv4.
- H.323 Devices—H.323 clients, gateways, and H.225 intercluster trunks do not support IPv6. To communicate with IPv6 Only devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.
- Intercom—Intercom can support phones with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. During an intercom call, the talkback mode establishes media streams with the same IP version as the media stream that is used when the caller initiated intercom.
- Mobile Connect and Mobile Voice Access—Cisco Unified Mobility features in Cisco Unified Communications Manager, such as Mobile Connect and Mobile Voice Access, support IPv4. On a call, when a mobile phone uses IPv4 and another phone uses IPv6, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 into the call.
- Monitoring and Recording—For monitoring and recording, the phone can handle an IPv4 media stream for customer-to-agent calls while it handles an IPv6 media stream for recording and monitoring (or vice versa).
- Music On Hold—The IP Voice Media Streaming Application supports IPv4. Cisco Unified Communications Manager does not support IPv6 with multicast music on hold, so devices with an IP Addressing Mode of IPv6 Only cannot support multicast music on hold. Under these circumstances, Cisco Unified Communications Manager plays a tone, instead of music, when the phone is on hold. For IPv6 Only devices that uses unicast music on hold, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa) into the media stream.

- QRT—The Quality Report Tool supports IPv6 if the device uses an IP Addressing Mode of IPv4 Only or IPv4 and IPv6 (dual-stack mode); users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only.
- RSVP—If you deploy RSVP as the call admission control mechanism in your network, do not deploy IPv6. The RSVP feature does not support IPv6. RSVP calls support IPv4. If RSVP is required for the call and any device in the call is configured for or uses an IPv6 address, Cisco Unified Communications Manager rejects the call, and the caller receives a busy tone.
- SDL—SDL TCP connections support IPv6, but SDL links support IPv4. If you configure a host name in the Server Configuration window in Cisco Unified Communications Manager Administration, SDL queries the DNS A record, which ensures that IPv4 is used. If you specify an IP address, an IPv4 address gets passed down to the SDL layer.
- SIP Phones and TFTP—Phones that run SIP do not support IPv6 addresses. If you configure IPv6 Only as the IP Addressing Mode for a phone that runs SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.
- T.38 Fax—Whether a T.38 fax call uses IPv4 or IPv6 depends on the preference of Cisco Unified Communications Manager and the capabilities of the devices in the call. If one device in the call uses IPv6 and the other device can use IPv4 and IPv6, the call uses IPv6, regardless of the configuration for the signaling and media enterprise parameters in Cisco Unified Communications Manager Administration.

  Cisco Unified Communications Manager supports the following types of T.38 fax calls:

  - SIP-to-SIP call that uses IPv6
  - SIP-to-SIP call that uses IPv4
  - SIP-to-non-SIP call that uses IPv4
  - SIP-to-non-SIP call where the SIP device uses IPv6 and the non-SIP device uses IPv4 with an MTP that can translate IP address versions

  During the middle of a T.38 fax call, Cisco Unified Communications Manager does not insert an MTP that converts the IP version types; the MTP must already exist in the call.
- Transfer—The transfer components in Cisco Unified Communications Manager uses the IP Addressing Mode and the IP address of the device to determine how to handle the transfer. If the IP capabilities do not match when you transfer a call, Cisco Unified Communications Manager allocates an MTP that can translate IP version, so the transfer can occur.
- Web Browser on the Phone—On the Cisco Unified IP Phone, the HTTP interface for the web browser supports IPv4 addresses, so the phone does not allow web access to servers that use an IPv6 address.
- Video—Cisco Unified Communications Manager supports video IPv6 calls in the following cases:
  - Cisco Unified Video Advantage does not support IPv6, so, when the media preference is IPv6, video uses IPv4.
  - The audio and video portions of a call negotiate the same IP type for the initial call; that is, if two dual-stack phones are in a call that uses both audio and video, the call uses IPv4 for both the audio and video portions of the initial call, even when the media preference is IPv6.
  - If two dual-stack phones negotiate IPv6 for the audio call based on the media preference and then you add video mid-call, the video portion of the call uses IPv4, even if the media preference is IPv6.

- MTPs do not get allocated for video support. For example, a call occurs between two dual-stack phones over a SIP trunk with an IP Addressing Mode of IPv6 Only; IPv6 gets negotiated for the audio portion of the call, and video cannot occur because the video device does not support IPv6. No MTP gets allocated to support the video portion of the call.

IPv6 Configuration Tips

Table 11 displays the configuration checklist for IPv6, which is documented in the "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. Before you configure IPv6 in your network, review Table 11.

Table 11 IPv6 Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 5	Before you configure IPv6, review all IPv6-related documentation.	For example, review the following documents: • *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)* • *Cisco IOS IPv6 Configuration Library* • *Implementing VoIP for IPv6* • "Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide*
Step 6	Make sure that you have compatible network hardware and Cisco IOS software that is installed and configured; for example, configure your gateways and Cisco IOS MTP for IPv6.	• *Implementing VoIP for IPv6* • "Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide*
Step 7	Provision a local IPv6-capable DNS and DHCP server. **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. **Tip** Cisco recommends that the Cisco Unified Communications Manager server use a static non-link-local IPv6 address. If the Cisco Unified Communications Manager server obtains the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration, ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address from the DHCPv6 server.	Refer to the documentation that supports your DNS and DHCP server(s); for example, *Cisco Network Registrar User's Guide, 6.2.*

Table 11 IPv6 Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 8	Install Cisco Unified Communications Manager 7.1 (or upgrade to this release). Before you install subsequent nodes (subscribers) in the cluster, add the IPv4 server information to the Server Configuration window in Cisco Unified Communications Manager Administration. ⚠ **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.	• Cisco Unified Communications Manager installation or upgrade 7.1 documentation • Configuring a Server, *Cisco Unified Communications Manager Administration Guide*
Step 9	Enable IPv6 in the Cisco Unified Communications Operating System and ensure that the Cisco Unified Communications Manager server obtains an IPv6 address. Cisco recommends that the Cisco Unified Communications Manager server use a static non-link-local IPv6 address. **Tip** For each server in the cluster, perform these tasks. Performing these tasks requires a reboot of the server.	"Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide* Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 70
Step 10	In the Enterprise Parameters Configuration window in Cisco Unified Communications Manager Administration, choose **True** for the Enable IPv6 enterprise parameter. **Tip** After you update this enterprise parameter, restart the Cisco CallManager, CTIManager and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.	"Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide* Service Parameter and Enterprise Parameter Changes for IPv6, page 78

Table 11 IPv6 Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 11	For the server that you are configuring in Cisco Unified Communications Manager Administration, choose **System > Server** and enter the non-link-local IPv6 address or a host name that can resolve to a IPv6 address in the IPv6 Name field. **Tip** For each server in the cluster, perform this task. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for IPv6 for Cisco Unified Communications Manager until after you upgrade to Release 7.1(2). Configuring the DNS records for IPv6 for Cisco Unified Communications Manager prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. To display the non-link-local IPv6 address, you can run a CLI command or view it in the Ethernet IPv6 window, as described in the "Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window" section on page 70.	• "Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide* • Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 73
Step 12	In Cisco Unified Communications Manager Administration, configure phone-related and SIP trunk-related IPv6 settings. For example, configure the IP Addressing Mode and Allow Auto-Configuration of Phones settings in the Common Device Profile Configuration window; then, apply the common device profile configuration to the phone or SIP trunk.	• "Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide* • Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 73
Step 13	Restart the Cisco CallManager, CTIManager, and Cisco Certificate Authority Proxy services in Cisco Unified Serviceability.	*Cisco Unified Serviceability Administration Guide*

Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window

To enable IPv6 in the Cisco Unified Communications Operating System and to ensure that the Cisco Unified Communications Manager server gets an IPv6 address, you must perform one of the following tasks:

- Run the IPv6 CLI commands in the command line interface.
- Enable IPv6 and configure the IPv6 address in the Ethernet IPv6 window in the Cisco Unified Communications Operating System.

Caution Before you set the Enable IPv6 enterprise parameter to True in Cisco Unified Communications Manager Administration, perform the following procedure. If you set the enterprise parameter to True before you enable IPv6 in the Cisco Unified Communications Operating System, the Cisco CallManager service runs in IPv4, and phones that have IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager.

Table 12 provides a description of the Ethernet IPv6 configuration settings and the equivalent CLI commands that support the graphical user interface (GUI) options.

Step 1 In Cisco Unified Communications Operating System, choose **Settings > IP > Ethernet IPv6**.

The Ethernet IPv6 Configuration window displays.

Step 2 To modify the Ethernet settings, enter the values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see Table 12.

Step 3 Check the **Update with Reboot** check box. For the IPv6 settings in this window to take effect, you must reboot the server.

Step 4 Click **Save**. The server reboots immediately after you click Save.

Step 5 Perform this procedure for each server in the cluster.

Table 12 IPv6 CLI Commands and Ethernet IPv6 Configuration Settings

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
Enable IPv6 check box	set network ipv6 service enable	These settings enable IPv6 in the Cisco Unified Communications Operating System. **Caution** For IPv6 to work, you must either check the Ethernet IPv6 check box or issue the equivalent CLI command. You must perform this task before you set the Enable IPv6 enterprise parameter to True.

Table 12 IPv6 CLI Commands and Ethernet IPv6 Configuration Settings (continued)

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
Router Advertisement radio button	Not applicable	If you want to use stateless address autoconfiguration to obtain a non-link-local IPv6 address for the Cisco Unified Communications Manager server, click the Router Advertisement radio button. Click this radio button if you do not plan to configure a static non-link-local IPv6 address for the Cisco Unified Communications Manager server or if you do not want DHCPv6 server to issue a non-link-local IPv6 address to the server. Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected. If the Cisco Unified Communications Manager server obtains an IPv6 address via stateless address autoconfiguration and you also have a static IPv6 address that is configured for the server, Cisco Unified Communications Manager ignores the IPv6 address that is obtained via stateless address autoconfiguration and uses the static address.
DHCP radio button	set network ipv6 dhcp enable	If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager server, click the DHCP radio button or issue the equivalent CLI command. Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.

Table 12 IPv6 CLI Commands and Ethernet IPv6 Configuration Settings (continued)

Configuration Setting in Ethernet IPv6 Window	Equivalent CLI Command	Description
Manual Entry radio button, IPv6 Address, Subnet Mask	set network ipv6 static_address <addr> <mask>	These Ethernet IPv6 settings and equivalent CLI command allow you to configure a static IPv6 address for the Cisco Unified Communications Manager server. Configuring a static non-link-local IPv6 address assumes that you do not want the Cisco Unified Communications Manager server to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration.
IPv6 Address	show network ipv6 settings	These settings allow you to view the IPv6 address for the Cisco Unified Communications Manager server.

Tip If you decide to run the CLI commands that are described in Table 12 instead of configure the Ethernet IPv6 settings in the Cisco Unified Communications Operating System, you must reboot the server for the changes to take effect. For information on how to run CLI commands and for other IPv6 CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Cisco Unified Communications Manager Administration IPv6 GUI Changes

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

Table 13 describes the IPv6 and IPv4 settings that are in Cisco Unified Communications Manager Administration. For some IPv6 settings in Table 13, equivalent settings for IPv4 display in Cisco Unified Communications Manager Administration; for example, in the SIP Trunk Configuration window, you can configure either the Destination Address IPv6 setting or the Destination Address setting, or both settings, depending on the IP support in your network.

For related configuration procedures, refer to the following sections:

- Service Parameter and Enterprise Parameter Changes for IPv6, page 78
- Configuring a Server, *Cisco Unified Communications Manager Administration Guide*
- Configuring a SIP Route Pattern, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Common Device Configuration, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide*

Table 13 IPv6 Settings in Cisco Unified Communications Manager Administration

Configuration Setting	Description
System > Server	
Host Name/IP Address	This field supports IPv4. If your network uses DNS that can map to IPv4 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, you must enter the full IPv4 address of the server. **Tip** If your network supports IPv6 (or IPv4 and IPv6), configure the IPv6 Name field in addition to the Host Name/IP Address field.
IPv6 Name	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the "Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window" section on page 70. Phones that run SCCP use this field, which gets included in the TFTP configuration file, to retrieve the IPv6 address of the Cisco Unified Communications Manager server, so phone registration occurs. **Tip** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. **Tip** In addition to configuring the IPv6 Name field, you must configure the Host Name/IP Address field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).
Call Routing > SIP Route Patterns	
IPv4 Pattern	Enter the domain, sub-domain, IPv4 address or IP subnetwork address. **Tip** For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, enter X.X.X.X/Y, where Y equals the network prefix that denotes the number of bits in the address that will be the network address. **Tip** If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.
IPv6 Pattern	Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. **Tip** If the SIP trunk supports both IPv4 and IPv6, configure the IPv4 Pattern in addition to the IPv6 Pattern.

Table 13 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Device > Device Settings > Common Device Configuration	
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to Cisco Unified Communications Manager. From the drop-down list box, choose one of the following options: • IPv4 Only—For both media and signaling events, the device uses an IPv4 address to connect to Cisco Unified Communications Manager. If an IPv4 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv6 address. If you choose this option, the SIP trunk uses an IPv4 address to connect to the peer device. • IPv6 Only—For both media and signaling events, the device uses an IPv6 address to connect to Cisco Unified Communications Manager. If an IPv6 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv4 address. If you choose this option, the SIP trunk uses an IPv6 address to connect to the peer device. Phones that run SIP do not support IPv6, so do not choose this option for these phones. If you configure IPv6 Only as the IP Addressing Mode for phones that run SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file. • IPv4 and IPv6 (Default)—Choose this option for dual-stack devices, which can have both an IPv4 and IPv6 address. For both media and signaling events, the dual-stack device uses either an IPv4 or an IPv6 address to connect to Cisco Unified Communications Manager. If only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call. If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events. From the drop-down list box, choose one of the following options: • IPv4—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event. • IPv6—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event. • Use System Default—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.

Table 13 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Allow Auto-Configuration for Phones	This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options: • On—Depending on how the M bit is set via stateless address autoconfiguration on the router, the phone can use the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address. Phones also require a TFTP server address to register with Cisco Unified Communications Manager. You can manually configure the TFTP server address via the interface on the phone, or you can obtain it from a DHCPv6 server. **Tip** To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O bit is set via stateless address autoconfiguration on the router. • Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server. • Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option. Although Cisco Unified Communications Manager does not use this configuration, the TFTP file that the phone obtains includes this information.
Device > SIP Trunk	
Destination Address	The Destination Address, which supports IPv4, represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV check box is checked. SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual-stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.

Table 13 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. Enter one for the following values in the field: • A valid IPv6 address (global unicast, unique local, or a host name) • A fully qualified domain name (FQDN) • A DNS SRV record, but only if you check the Destination Address is an SRV check box. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field.
Device > Device Settings > SIP Profile	
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the Media Termination Point Required check boxes, Cisco Unified Communications Manager inserts a dual-stack MTP and sends out an offer with two m-lines, one for IPv4 and another for IPv6. If a dual- stack MTP cannot be allocated, Cisco Unified Communications Manager sends an INVITE without SDP. When you check the Enable ANAT check box and the Media Termination Point Required check box is unchecked, Cisco Unified Communications Manager sends an INVITE without SDP. When both the Enable ANAT and Media Termination Point Required check boxes display as unchecked (or when an MTP cannot be allocated), Cisco Unified Communications Manager sends an INVITE without SDP. When you uncheck the Enable ANAT check box but you check the Media Termination Point Required check box, consider the information, which assumes that an MTP can be allocated: • Cisco Unified Communications Manager sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Cisco Unified Communications Manager sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Cisco Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.

Service Parameter and Enterprise Parameter Changes for IPv6

Table 14 describes the enterprise and service parameters that you can configure for IPv6. To configure enterprise parameters in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. To configure service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**.

Tip For a step-by-step procedure on how to configure enterprise parameters, refer to the "Enterprise Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For a step-by-step procedure on how to configure service parameters, refer to the "Service Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Table 14 Enterprise and Service Parameters for IPv6

Parameter	Description
Enable IPv6	This enterprise parameter specifies whether Cisco Unified Communications Manager can negotiate calls by using IPv6 and whether phone can advertise an IPv6 address. Before you set this parameter to **True**, make sure that you enabled IPv6 in the Cisco Unified Communications Operating System on all servers in the cluster. Setting this parameter to **True** causes the Cisco CallManager service to run in dual-stack mode, which is required for interacting with devices that support IPv6. The default value equals False, which means that Cisco Unified Communications Manager cannot negotiate calls by using IPv6 and phones cannot advertise an IPv6 address. After you update this enterprise parameter, restart the Cisco CallManager, CTIManager, and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.
IP Addressing Mode Preference for Media	This enterprise parameter, which applies only to dual-stack devices, specifies the addressing mode that Cisco Unified Communications Manager uses for media events when both IPv4 and IPv6 addresses are available from each device on the call. The default value equals Prefer IPv4.
IP Addressing Mode Preference for Signaling	This enterprise parameter, which applies only to dual-stack devices, specifies how the dual-stack phone connects to Cisco Unified Communications Manager for signaling events and how the dual-stack SIP trunk connects to the peer device for signaling events. The default value equals Prefer IPv4.
Allow Auto-Configuration for Phones	This parameter determines whether the phone is allowed to obtain an address through stateless autoconfiguration. Valid values specify On (the phone obtains its address as specified by the router advertisements, which may be stateless or stateful, depending on the router configuration) or Off (the phone always uses DHCPv6 to obtain its IPv6 address).

Table 14 Enterprise and Service Parameters for IPv6 (continued)

Parameter	Description
Call Counting CAC Enabled	This service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager uses call counting as part of the locations-based call admission control (CAC) feature. Call counting uses a fixed bandwidth value to reserve and adjust bandwidth per call, regardless of the codec or media payload or the Internet Protocol Version (IPv6 or IPv4) that is used for each call. Call counting may potentially oversubscribe or undersubscribe bandwidth because a fixed-value bandwidth gets reserved per call no matter what the actual bandwidth is for the call. Cisco recommends you leave this parameter set to the default value of **False** (disabled) unless your network requires the call counting feature. To enable call counting for CAC, choose **True** for the parameter; to disable call counting for CAC, choose **False**. This service parameter applies to IPv4 and IPv6 calls.
Audio Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the amount of bandwidth to deduct from the available bandwidth for audio calls after you set the Call Counting CAC Enabled parameter to **True**. For each audio call, the amount of bandwidth that you enter in this field gets deducted, regardless whether more or less bandwidth is actually used for the call. This service parameter applies to IPv4 and IPv6 calls.
Video Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the units of bandwidth to deduct from the available bandwidth for video calls after you set the Call Counting CAC Enabled parameter to **True**. For each video call, the available bandwidth gets reduced by the number of units that are required to account for the actual bandwidth usage. For example, if you specify 512 kb/s as the bandwidth unit in this parameter, and a video call utilizes 384 kb/s, then one unit, 512 kb/s, gets deducted from available bandwidth. Likewise, if you specify 512 kb/s in this parameter and a video call negotiated 768 kb/s, then two units of bandwidth (1064 kb/s) get deducted from the available bandwidth. This service parameter applies to IPv4 and IPv6 calls.
Alternate Cisco File Server(s)	These service parameters, which support the Cisco TFTP service, allow you to configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.

Installation/Upgrade (Migration) Considerations for IPv6

Cisco Unified Communications Manager supports IPv6 after you install 7.1(2) or upgrade to 7.1(2).

⚠ **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

For additional considerations, see Table 11 on page 68.

Serviceability and RTMT Considerations for IPv6

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, refer to the *Cisco Unified Serviceability Administration Guide*. The following alarms may provide IPv6 information.

- kCtiProviderOpenFailure (Updated)
  - The alarm indicates that the CTI application failed to open provider. If your network supports IPv6, this alarm may contain an IPv6 address.
  - Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
  - Severity—Error (3)
  - New Parameter—IPV6Address(String)
- kCtiProviderClosed (Updated)
  - The alarm indicates that the CTI application connection is closed. If your network supports IPv6, this alarm may contain an IPv6 address.
  - Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
  - Severity—Informational (6)
  - New Parameter—IPV6Address(String)
- kCtiProviderOpened (Updated)
  - The alarm indicates that the CTI application connection opened. If your network supports IPv6, this alarm may contain an IPv6 address.
  - Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
  - Severity—Informational (6)
  - New Parameter—IPV6Address(String)
- kCtiIncompatibleProtocolVersion (Updated)
  - The alarm indicates that the JTAPI/TAPI application version is not compatible with this version of CTIManager. If your network supports IPv6, this alarm may contain an IPv6 address.
  - Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
  - Severity—Error (3)
  - New Parameter—IPV6Address(String)
- DeviceRegistered (Updated)
  - A device successfully registered with Cisco Unified Communications Manager.
  - Alarm Definition Catalog—Choose CallManager Alarm Catalog > CallManager.
  - Severity—Informational (6)

  - New Parameters—IPV6Address[Optional].[String], IPAddressAttributes[Optional].[Enum], IPV6AddressAttributes [Optional].[Enum], ActiveLoadId [Optional].[String]
  - New Enum Definitions for IPAddrAttributes: 0—Unknown; 1—Administrative only; 2—Signal only; 3—Administrative and signal
  - New Enum Definitions for IPV6AddrAttributes: 0—Unknown; 1—Administrative only; 2—Signal only; 3—Administrative and signal
- DeviceUnregistered (Updated)
  - A device that was previously registered with Cisco Unified Communications Manager has unregistered. This event may get issued as part of normal unregistration event or due to some other reason such as loss of keepalives. In cases of normal unregistration, if the Reason Code is CallManagerReset, CallManagerRestart, or DeviceInitiatedReset, the alarm severity gets lowered to Informational (6).
  - Alarm Definition Catalog—Choose CallManager Alarm Catalog > CallManager.
  - Severity—Error (3)
  - New Parameters—IPV6Address [Optional].[String], IPAddressAttributes [Optional].[Enum], IPV6AddressAttributes [Optional].[Enum]
  - New Enum Definitions for IPAddrAttributes: 0—Unknown; 1—AdministrativeOnly; 2—SignalOnly; 3—AdministrativeAndSignal
  - New Enum Definitions for IPV6AddrAttributes: 0—Unknown; 1—Administrative only; 2—Signal only; 3—Administrative and signal
- DeviceTransientConnection (Updated)
  - A transient connection attempt occurred. A connection got established and immediately dropped before completing registration. Incomplete registration may indicate a device is rehoming in the middle of registration. The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.
  - Alarm Definition Catalog—CallManager Alarm Catalog > CallManager
  - Severity—Error (3)
  - New Parameters—IPV6Address [Optional].[String], IPAddressAttributes [Optional].[Enum], IPV6AddressAttributes [Optional].[Enum]
  - Enum Definitions for IPAddrAttributes: 0—Unknown; 1—AdministrativeOnly; 2—SignalOnly; 3—AdministrativeAndSignal
  - Enum Definitions for IPV6AddrAttributes: 0—Unknown; 1—AdministrativeOnly; 2—SignalOnly; 3—AdministrativeAndSignal

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

With Release 7.1(2), the CTI InetAddress ccmCTIDeviceInetAddressType and ccmCTIDeviceInetAddress fields get deprecated. Two new IPv4/IPv6 fields get added to improve the SNMP query performance when a huge number of entries exist in the table.

The new fields that are added to the ccmCTIDeviceTable in CISCO-CCM-MIB comprise ccmCTIDeviceInetAddressIPv4 and ccmCTIDeviceInetAddressIPv6.The definitions follow:

```
ccmCTIDeviceInetAddressIPv4 OBJECT-TYPE
SYNTAX          InetAddressIPv4
MAX-ACCESS      read-only
```

```
STATUS                  current
DESCRIPTION—This object identifies the last known primary IPv4 address of the CTI device. This
object contains value zero if IPV4 address is not available.
::= { ccmCTIDeviceEntry 14 }


ccmCTIDeviceInetAddressIPv6 OBJECT-TYPE
SYNTAX          InetAddressIPv6
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION—This object identifies the last known primary IPv6 address of the CTI device. This
object contains value zero if IPV6 address is not available.
::= { ccmCTIDeviceEntry 15 }
```

With these changes, the ccmCTIDeviceEntry looks like the following example:

```
CcmCTIDeviceEntry ::= SEQUENCE {
    ccmCTIDeviceIndex                   CcmIndex,
    ccmCTIDeviceName                    SnmpAdminString,
    ccmCTIDeviceType                    INTEGER ,
    ccmCTIDeviceDescription             SnmpAdminString,
    ccmCTIDeviceStatus                  CcmDeviceStatus,
    ccmCTIDevicePoolIndex               CcmIndexOrZero,
    ccmCTIDeviceInetAddressType         InetAddressType,
    ccmCTIDeviceInetAddress             InetAddress,
    ccmCTIDeviceAppInfo                 SnmpAdminString,
    ccmCTIDeviceStatusReason            CcmDevFailCauseCode,
    ccmCTIDeviceTimeLastStatusUpdt      DateAndTime,
    ccmCTIDeviceTimeLastRegistered      DateAndTime,
    ccmCTIDeviceProductTypeIndex        CcmIndexOrZero,
    ccmCTIDeviceInetAddressIPv4         InetAddressIPv4,
    ccmCTIDeviceInetAddressIPv6         InetAddressIPv6
}
```

In RTMT, you can search for and monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the application, device, or line, enter the IPv6 address and check the AppIpv6Addr check box in the attribute window.

In addition, you can perform a device search for phones or SIP trunks that use IPv6 addresses. When you choose **CallManager > Device Search > Open Device Search > Phones** (or **SIP Trunks**), make sure that you specify an IPv6 address and check the IPv6Address check box in the attributes window.

Tip IP Subnet does not apply for IPv6 search criteria.

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

CAR/CDR Considerations for IPv6

Cisco Unified Communications Manager 7.1(2) supports the new IPv6-related CDR fields in Table 15.

Table 15 IPv6 CDR Field Descriptions

Field Name	Range of Values	Description
origIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that originates the call signalling. The field represents either IPv4 or IPv6 format depending on the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field specifies the address of the Cisco Unified IP Phone. For PSTN calls, this field specifies the address of the gateway. For intercluster calls, this field specifies the address of the remote Cisco Unified Communications Manager. The IP address displays either in dotted decimal format or in colon-separated hexadecimal format. Default - This field represents the IP address of the originating device as reported by the device or used for the call after media negotiation.
destIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that terminates the call signalling. The field can represent either IPv4 or IPv6 format depending on the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field specifies the address of the Cisco Unified IP Phone. For PSTN calls, this field specifies the address of the gateway. For intercluster calls, this field specifies the address of the remote Cisco Unified Communications Manager. The IP address displays either in dotted decimal format or in colon-separated hexadecimal format. Default - Empty String "" or null represents the default. If the destination does not get reached, this field stays empty.

Security Considerations for IPv6

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. Table 16 describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 16 How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv6	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv4	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6	IPv6	IPv4	Phone cannot connect to CAPF.

AXL and CTI Considerations

See the following sections:

- IPv6 Support, page 176
- IPv6 Support, page 178
- IPv6 Support, page 181
- IPv6 Support, page 183

Supported Phone Models for IPv6

The following Cisco Unified IP Phones that run SCCP support IPv6:

- 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

Phone Considerations

The Cisco Unified IP Phone uses the internet protocol to provide voice communication over the network. Previous to Cisco Unified Communications Manager Release 7.1(x), only the internet protocol version 4 (IPv4) got supported. Because it uses a 32-bit address, IPv4 cannot meet the increased demands for unique IP addresses for all devices that can connect to the Internet. Internet Protocol version 6 (IPv6) represents an updated version of the current Internet Protocol, IPv4. IPv6 uses a 128-bit address and provides end-to-end security capabilities, enhanced Quality of Service (QoS), and increased number of available IP addresses.

The Cisco Unified IP Phone can support an IP Addressing Mode of IPv4 Only, IPv6 Only, or IPv4 and IPv6 in dual stack mode, as configured in Cisco Unified Communications Manager Administration. In IPv4, you can enter each octet of the IP address on the phone in dotted decimal notation; for example, 192.240.22.5. In IPv6, you can enter each octet of the IP address in hexadecimal notation with each octet separated by a colon; for example, 2005:db8:0:1:ef8:9876:ba72:dc9a. The phone truncates and removes leading zeros when it displays the IPv6 address.

Cisco Unified IP Phones support both IPv4 and an IPv6 address transparently, so users can handle all calls on the phone to which they are accustomed. Cisco Unified IP Phones support the use of IPv6 only with Cisco Unified Communications Manager Release 7.1(x) and only with the Skinny Call Control Protocol (SCCP).

Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This affects all IP Phone Service URLs, including services, directories, messages, help, and any restricted web services that require the phone to use HTTP to validate the credentials with the Authentication URL. If you configure Cisco Unified IP Phone services for Cisco Unified IP Phones, you must configure the phone and the servers that support the phone service with IPv4 addresses.

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

Table 17 describes the networking protocols on the Cisco Unified IP Phone and whether the protocols support IPv6.

Table 17 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Hypertext Transfer Protocol (HTTP)	HTTP represents the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes. Cisco Unified IP Phones do not support the use of IPv6 addresses in the URL. You cannot use a literal IPv6 address in the URL or a hostname that maps to an IPv6 address.
Internet Protocol (IP)	IP, a messaging protocol, addresses and sends packets across the network.	To communicate by using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications automatically get assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phone supports concurrent IPv4 and IPv6 addresses. Configure the IP addressing mode (IPv4 only, IPv6 only, and both IPv4 and IPv6) in Cisco Unified Communications Manager Administration. For more information, refer to the “Internet Protocol Version 6 (IPv6)” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Session Initiation Protocol (SIP)	SIP represents the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP, an ASCII-based application-layer control protocol (defined in RFC 3261), can get used to establish, maintain, and terminate calls between two or more endpoints.	SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows call information to get carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support SIP when the phones are operating in IPv6 address mode.

The following section provides information on how DHCP and Autoconfiguration affects the network settings on the phone. You can choose to configure the IP address and other network settings, such as the TFTP server, DNS server, domain, name, and so on, on an IP phone manually or by using a router and/or a DHCP server to automatically assign the IP address and other network information. For more information on how the Auto IP Configuration and DHCPv6 settings determine where the IP phone acquires its IPv6 address and other network settings, see Table 18.

Tip If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after you install the phone on the network:

IP address

IP subnet information (subnet mask for IPv4 and subnet prefix length for IPv6)

Table 18 Determining Where a Phone Acquires Its Network Settings

DHCPv6	Auto IP Configuration	How the Phone Acquires Its IP address and Network Settings
Disabled	Disabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting gets ignored.
Disabled	Enabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting gets ignored.
Enabled	Disabled	The DHCP server assigns the IP address and the other network settings to the phone.
Enabled	Enabled	When the M-bit is set on the router, the O-bit gets ignored. The phone can set its IPv6 address based on an IPv6 address that it received from a DHCPv6 server, or the phone can acquire its IPv6 address through stateless address autoconfiguration. When the M-bit is not set, you should set the O-bit on the router. The phone will then acquire its IPv6 address through stateless address autoconfiguration. It will not request an IPv6 address from the DHCPv6 server, but it will request other network configuration information.

Table 19 describes the phone menus that relate to IPv4 and IPv6. When you edit the value of an option setting on the phone, follow these guidelines:

- To enter a period (for example, in an IP address under IPv4 Configuration), press the **.** (period) softkey or press ***** on the keypad.
- To enter a colon (for example, in an IP address under IPv6 Configuration), press the : (colon) softkey or press * on the keypad.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu		
IPv4 Configuration	Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following tasks: • Enable or disable the phone to use the IPv4 address that is assigned by the DHCPv4 server. • Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4. For more information on the IPv4 address fields, refer to the specific field within this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv4 Configuration and press the **Select** softkey.
IPv6 Configuration	Internet Protocol v6 address menu. In the IPv6 Configuration menu, you can do the following tasks: • Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server or to use the IPv6 address that it acquires through Stateless Address Autoconfiguration (SLAAC). • Manually set the IPv6 Address, Subnet Prefix Length, DNSv6 Server, and IPv6 TFTP servers. For more information on the IPv6 address fields, refer to the specific field within this table. For more information on SLAAC, refer to *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)*.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv6 Configuration and press the **Select** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides. **Note** If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 server will take precedence.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Disable DHCP. If the IP Addressing mode is configured for IPv4 only, set the DHCP option to **No**. If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to **No**. If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to **No**. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
Settings > Network Configuration Menu > IPv4 Configuration Menu		
DHCP	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone anIPv4 address. When DHCP is disabled, the administrator must manually assign an IPv4 address to the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP option and press the **No** softkey to disable DHCP or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Address	Internet Protocol version 4 (IPv4) address of the phone. If you assign an IPv4 address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
Subnet Mask	Subnet mask that the phone uses.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router that the phone uses (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) that the phone uses.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IPv4 address.	Display only—Cannot configure.
DHCP Address Released	Releases the IPv4 address that the DHCP server assigned.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address that is assigned by DHCP or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server that is used by the phone with an IPv4 address. If you are not using DHCPv4 in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to **Yes** or disable DHCP, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. A new CTL file will get downloaded from the new TFTP Server 1 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order in which it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Any manually assigned IPv6 TFTP Servers 2. Any manually assigned IPv4 TFTP Servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCP is enabled, set the Alternate TFTP option to Yes. 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 2	Optional backup TFTP server that the phone with an IPv4 address uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. A new CTL file will get downloaded from the new TFTP Server 2 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order in which it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey and then press the **Save** softkey.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu > IPv6 Configuration Menu		
DHCPv6	Indicates whether the phone has DHCPv6 enabled or disabled. When DHCPv6 is enabled, the DHCPv6 server assigns an IPv6 address to the phone. When DHCP v6 is disabled, the administrator must manually assign an IPv6 address to the phone. The DHCPv6 setting, along with the Auto IP Configuration setting, determine how the phone obtains its network settings. For more information on how these two settings affect the network settings on the phone, see Table 18 (Determining Where a Phone Acquires its Network Settings).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 option and press the **No** softkey to disable DHCPv6 or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.
IPv6 Address	Internet Protocol version 6 (IPv6) address of the phone. The IPv6 address comprises a 128-bit address. If you assign an IP address with this option, you must also assign the IPv6 prefix length. See the IPv6 Subnet Prefix options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
IPv6 Prefix Length	Subnet prefix length that the phone uses. The subnet prefix length specifies a decimal value from 1-128, which specifies the portion of the IPv6 address that comprises the subnet.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IPv6 Prefix Length option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Default Router 1	Default router (Default Router 1) that the phone uses. **Note** The phone obtains information on the default router from IPv6 Router Advertisements.	Display only—Cannot configure.
IPv6 DNS Server 1 IPv6 DNS Server 2	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2) that the phone uses. If your configuration includes both DNSv6 and DNSv4 servers, the phone will look for its DNS server in the following order: 1. IPv6 DNS Server 1 2. IPv6 DNS Server 2 3. DNS Server 1-5 for IPv4 (respectively)	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign the backup DNS server. 6. Press the **Save** softkey.
DHCPv6 Address Released	Releases the IPv6 address that the phone acquired from the DHCPv6 server or by stateless address autoconfiguration. **Note** You can only edit this field when the DHCPv6 option is enabled.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 Address Released option and press the **Yes** softkey to release the IP address that is assigned by DHCP or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the IPv6 Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 1 (for phones that are running SCCP only)	Primary IPv6 Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCPv6 in your network and you want to change this server, you must use the IPv6 TFTP server 1 option. If you set the IPv6 Alternate TFTP option to **Yes** or you disable DHCPv6, you must enter a non-zero value for the IPv6 TFTP server 1 option. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order in which it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the “Security Configuration Menu” section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCPv6 is enabled, set the IPv6 Alternate TFTP option to **Yes**. 3. Scroll to the IPv6 TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 2 (for phones that are running SCCP only)	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order in which it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the IPv6 TFTP Server 1 option. 4. Scroll to the IPv6 TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey and then press the **Save** softkey.
Settings > Device Configuration > Network Configuration Menu		
IP Addressing Mode	Displays the IP addressing mode that is available on the phone—IPv4 only, IPv6 only, or Both (IPv4 and IPv6).	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are available on the phone. Displays one of the following options on the phone: • IPv4—The dual-stack phone prefers to establish a connection via an IPv4 address during a signaling event • IPv6—The dual-stack phone prefers to establish a connection via an IPv6 address during a signaling event.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.
Auto IP Configuration	Displays whether the auto configuration is enabled or disabled on the phone. The Auto IP Configuration setting, along with the DHCPv6 setting, determine how the phone obtains its IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see Table 18 (Determining Where a Phone Acquires its Network Settings). **Note** Use the "Allow Auto-Configuration for Phones" setting in Cisco Unified Communications Manager Administration.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, which negates the need to traverse the WAN link for each upgrade of the phone. You can set the Load Server to another TFTP server IP address or name (other than the IPv6 TFTP Server 1 or IPv6 TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use IPv6 TFTP Server 1 or IPv6 TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion. **Note** When you configure both an IPv6 Load Server and a Load Server (for IPv4), the IPv6 Load Server takes precedence.	Use Cisco Unified Communications Manager Administration to modify.
IPv6 Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer-to-peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages that are sent to the phone log.	Use Cisco Unified Communications Manager Administration to modify.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Settings > Security Configuration Menu		
CAPF Server	Displays the Common Name (from the Cisco Unified Communications Manager Certificate) and the port of the IPv4 CAPF server that the phone uses.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.
IPv6 CAPF Server	Displays the IP address and the port of the IPv6 CAPF server that the phone uses.This menu setting gets disabled in this release. If your configuration includes both IPv6 CAPF server and IPv4 CAPF server, the phone will look for its CAPF server in the following order: 1. IPv6 CAPF Server 2. IPv4 CAPF Server	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.

Table 19 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Settings > Status > Network Statistics		
IPv6	This includes the following states: • DHCP6 BOUND; • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DHCP6 DECLINED DUPLICATE IP • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT. CANNOT RESTORE • STACK TURNED OFF	Displays information on the DHCPv6 status.

For More Information

- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)*
- *Cisco IOS IPv6 Configuration Library*
- *Implementing VoIP for IPv6*
- “Internet Protocol Version (IPv6)” chapter, *Cisco Unified Communications Manager Features and Services Guide*

Licensing Enhancements

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce these licensing enhancements.

Description

Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) identify the state of a license; that is, if it is missing, if it is a demo license, or if it is an uploaded license. In addition, Cisco Unified Communications Manager Administration warns you whether Cisco Unified Communications Manager currently operates with demo licenses, with an insufficient number of licenses, or with an incorrect software feature license.

Cisco Unified Communications Manager Administration Configuration Tips

For information on how to configure licensing, refer to the licensing chapters in the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager Security Guide*.

GUI Changes

The following windows display the state of licenses in Cisco Unified Communications Manager Administration:

- Main Window—After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For example, Cisco Unified Communications Manager may identify the following situations:
  - Cisco Unified Communications Manager currently operates with demo licenses, so upload the appropriate license files.
  - Cisco Unified Communications Manager currently operates with an insufficient number of licenses, so upload additional license files.
  - Cisco Unified Communications Manager does not currently use the correct software feature license. In this case, the Cisco CallManager service stops and does not start until you upload the appropriate software version license and restart the Cisco CallManager service.
- License File Upload (System > Licensing > License File Upload)—This window displays a message that uploading the license file removes the demo licenses for the feature.
- License Unit Report (System > Licensing > License Unit Report)—This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded.

Service Parameter and Enterprise Parameter Changes

No service parameters or enterprise parameters considerations exist for these licensing enhancements.

Installation/Upgrade (Migration) Considerations

After you upgrade to Cisco Unified Communications Manager 7.1(2) from a compatible Cisco Unified CM 5.X or 6.X release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated.

Immediately after you complete the upgrade to Cisco Unified Communications Manager 7.1(2), upload the software feature license that is required for Cisco Unified Communications Manager 7.1(2) in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 7.1(2).

Serviceability Considerations

After you upload a license file, you must restart the Cisco CallManager service for the changes to take effect.

BAT Considerations

No BAT considerations exist for these licensing enhancements.

CAR/CDR Considerations

No CAR or CDR considerations exist for these licensing enhancements.

Security Considerations

No security considerations exist for these licensing enhancements.

AXL and CTI Considerations

No AXL or CTI considerations exist for these licensing enhancements.

User Tips

This feature does not impact the end user.

For More Information

- “Licensing” chapter, *Cisco Unified Communications Manager System Guide*
- Use Microsoft Outlook to Receive Cisco Unified Communications Manager Licenses, page 16

Location-Based Call Admission Control Over Intercluster Trunk

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

When a call is made across cluster through an intercluster trunk (ICT) and gets hairpinned back to the same location or site of the same cluster, although the media is exchanged between two endpoints in the same site or location, the current design of Cisco Unified Communications Manager location call admission control (CAC) deducts location bandwidth twice, once for the outbound call and again for the inbound call. The result does not correctly reflect the bandwidth consumption, which eventually causes denial of a new call to or from the site or location.

To resolve the bandwidth calculation problem, this feature enables Cisco Unified Communications Manager to pass location information, the primary key ID (PKID) of location record and location name, as a proprietary information element (IE) between the calling and called parties through an ICT, either in the H.323 protocol or SIP. Thus, either endpoint knows the true location information of the party/endpoint, not the location information of the ICT.

Currently Cisco Unified Communications Manager has Hub_None as the default location that has unlimited bandwidth, plus any user-created location to which the user can assign a device and for which the user can configure bandwidth.

A new type of Cisco Unified Communications Manager location gets created specifically for the ICT for this type application. This new type of location, designated as the Phantom location, also has unlimited bandwidth. The locations server does not deduct bandwidth for a device that is assigned to the Phantom location. A device, such as the ICT, that is assigned to the Phantom location can use its own location or the true location of the connected device. Likewise, the outbound ICT can use its own location or the callee location, and the inbound ICT can use its own location or the caller location to deduct or adjust the bandwidth.

When the media connect, Cisco Unified Communications Manager adjusts the allocated location bandwidth according to the negotiated media codec. Cisco Unified Communications Manager can correctly readjust the location bandwidth based on received callee location information for the outbound call. This enhancement helps the outbound call, which has reserved bandwidth during call setup time, to adjust the bandwidth back to 0 if the call is hairpinned back to the same site or location.

Some supplementary services, such as transfer, can also hairpin the call back to the same site or location after the initial call setup process. Be aware that passing the location information of the final destination through the Notify signals (H.323) and re-INVITE signals (SIP) back to the calling cluster, so bandwidth can be adjusted to the right value, is also required.

Because location record PKID is uniquely defined within the Cisco Unified Communications Manager enterprise environment, Cisco Unified Communications Manager uses location record PKID to identify whether the call over ICT has been looped back to the same cluster for the location-based CAC purpose. If other applications, like Cisco Voice Proxy (CVP), that do not have access to the Cisco Unified Communications Manager database for location record PKID information and also because PKID is a string of characters and digits, applications may need to rely on the location name information being passed around for the purpose of CAC. The same location name may exist for different locations with different location PKIDs in two different Cisco Unified Communications Manager clusters, which may cause confusion to the applications.

Cisco Unified Communications Manager Administration Configuration Tips

The Location Configuration window specifies the Phantom location as a location, besides the Hub_None location, that can be selected. Administrators cannot delete the Phantom location.

Administrators can create a new default location for the new Phantom location, similar to the Hub_None location. The Phantom location includes unlimited audio and video bandwidth value, and the administrator cannot modify the audio and video bandwidth values. The user can assign a location-pair RSVP policy between this new location and other existing locations.

Tip If the intercluster trunk or H.323 gateways gets configured in any other location besides the Phantom location, this feature does not work. In addition, if the intercluster trunk is connected to a third-party system that does not recognize and pass the Cisco-specific location information in the SIP or H.323 signals, this feature does not work.

GUI Changes

This feature does not entail any new menu options or new fields in Cisco Unified Communications Manager Administration. The Phantom value gets added for all entities that specify a location in the Location drop-down list box. The Location field displays in the Device Pool Configuration, Annunciator Configuration, Music On Hold (MOH) Server Configuration, Conference Bridge Configuration, Voice

Mail Port Configuration, Voice Mail Port Wizard Configuration, CTI Route Point Configuration, Gateway Configuration, Phone Configuration, Trunk Configuration, and Pilot Point Configuration windows.

Service Parameter and Enterprise Parameter Changes

No service parameter nor enterprise parameter changes apply to this feature.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager maintains the RSVP policy for the Phantom location during migration.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL nor CTI considerations exist for this feature.

User Tips

This feature does not entail user interaction.

For More Information

- Call Admission Control, *Cisco Unified Communications Manager System Guide*
- Resource Reservation Protocol, *Cisco Unified Communications Manager System Guide*
- Understanding Cisco Unified Communications Manager Trunk Types, *Cisco Unified Communications Manager System Guide*
- Location Configuration, *Cisco Unified Communications Manager Administration Guide*

Logging Missed Calls for Shared Lines

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

With the missed call logging for shared lines feature, the administrator can configure Cisco Unified Communications Manager Administration, or the phone user can configure Cisco Unified CM User Options, so Cisco Unified Communications Manager logs missed calls in the call history to a specified shared-line appearance on a phone.

Tip If configured correctly, this feature works if a phone user logs in to a phone via Cisco Extension Mobility.

The examples in Table 20, which use the following phones, describe how the missed call logging feature works for shared lines:

- Phone A, which has directory number 1000 that is configured for the first line and directory number 2000 for the second line, which is shared with phone B.
- Phone B, which has directory number 2000 that is configured as the first line, which is shared with phone A, and directory number 3000 configured as the second line.
- Phone C, which places the calls.

Table 20 Example of How Logging Works for Missed Calls With Shared Lines

Phone A	Phone B
• Phone C calls directory number (DN) 1000. • The Logged Missed Calls check box is checked for DN 1000. • Missed calls get logged to DN 1000. If the Logged Missed Calls check box is not checked, missed calls do not get logged to DN 1000.	Not applicable
• Phone C calls directory number (DN) 2000. • The Logged Missed Calls check box is checked for DN 2000. • Missed calls get logged to DN 2000. If the Logged Missed Calls check box is not checked, missed calls do not get logged to DN 2000.	• Phone C calls DN 2000, which is a shared line appearance. • Logging displays for the shared line appearance on Phone B because the Logged Missed Calls check box is checked for DN 2000.

Cisco Unified Communications Manager Administration Configuration Tips

If this feature is not configured, the call history on the phone does not display missed calls for the specified line appearance.

GUI Changes

If the phone supports this feature, the Directory Number Configuration window in Cisco Unified Communications Manager Administration displays the Log Missed Calls check box, which allows you to turn on or off this feature. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone. To access the Directory Number Configuration window, choose **Call Routing > Directory Number**.

The Directory Number Configuration window in Cisco Unified Communications Manager Administration displays the Logged Missed Calls check box, which turns this feature on or off. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone. To access the check box, choose **Call Routing > Directory Number**. In the Directory Number Configuration window, highlight the associated device in the Associated Devices pane; then, click the **Edit Line Appearance** button.

In the Line Settings Configuration window in the Cisco Unified CM User Options, the phone user can check and uncheck the Log Missed Calls check box.

Service Parameter and Enterprise Parameter Changes

No new or updated parameters exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(2) or upgrade to 7.1(2), you can configure this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

The Bulk Administration GUI includes the following updates to support the Log Missed Calls feature:

- Log Missed Calls Check Box— This check box allows you to turn this feature on or off. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone.

Note The Log Missed Calls Check Box displays in the Phone Line Template, UDP Line Template, Phone Update Line, and UDP Update Line windows.

- Insert, Export, and Validate Details support for the log missed calls feature—The following insert, export, and validate details features have support for the log missed calls feature:
  - 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
- File Formats—The following file formats support the Log Missed Calls feature:

  - Phone File Format—Log Missed Calls field exists as a part of the Line Fields section.
  - UDP File Format—Log Missed Calls field exists as a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Log Missed Calls field in the Line Fields section.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

Tip If configured correctly, this feature works when a Cisco Extension Mobility user logs in to a phone via Cisco Extension Mobility.

For a list of phone models that support this feature, see the "Missed Calls" section on page 189.

For More Information

- Missed Calls, page 189

Logical Partitioning

This section, which describes logical partitioning support for Cisco Unified Communications Manager 7.1(2), contains information on the following topics:

- Description of Logical Partitioning, page 111
  - Identifiers for Logical Partitioning, page 112
  - Allow and Deny Policies for Logical Partitioning, page 112
- Cisco Unified Communications Manager Administration Configuration Tips for Logical Partitioning, page 112
- Interactions and Limitations for Logical Partitioning, page 115
- GUI Changes for Logical Partitioning, page 117
- Service Parameter and Enterprise Parameter Changes for Logical Partitioning, page 118
- Installation/Upgrade (Migration) Considerations for Logical Partitioning, page 118
- Serviceability Considerations for Logical Partitioning, page 119
- BAT Considerations for Logical Partitioning, page 119
- CAR/CDR Considerations for Logical Partitioning, page 119
- Security Considerations for Logical Partitioning, page 119
- AXL and CTI Considerations for Logical Partitioning, page 120
- For More Information About Logical Partitioning, page 120

Description of Logical Partitioning

The Logical Partitioning feature specifies the capability of a telephony system to control calls and features on the basis of specific allowed or forbidden configurations. A common telephony system can provide access to Voice over Internet Protocol (VoIP) and Public Switched Telephone Networks (PSTN), and configuration can control access.

Logical partitioning specifies a call control feature in Cisco Unified Communications Manager that provides functionality, so communication between the following pairs of VoIP entities can be controlled:

1. A VoIP phone and a VoIP gateway
2. A VoIP gateway and another VoIP gateway
3. An intercluster trunk and a VoIP phone
4. An intercluster trunk and a VoIP gateway

Options exist to configure Cisco Unified Communications Manager, so any such set of VoIP devices may be allowed communication with each other and any device can be restricted to one device or to a group of devices. No logical partitioning policy logic exists on endpoints.

Be aware that logical partitioning is required to control such communication not only during basic call establishment but also during mid-call as a result of midcall features.

The Cisco Unified Communications Manager basic routing policy constructs of calling search spaces and partitions suffice to prevent forbidden basic calls from being established but are not sufficient to prevent forbidden calls from being created as a result of midcall features. In Cisco Unified Communications Manager, such midcall features often get termed Join and Redirect features, because these primitives often get used internally to affect these features.

Logical partitioning enhances Cisco Unified Communications Manager to handle such midcall scenarios. Configuration for logical partitioning remains independent of supplementary features, where the policy checking gets performed based on devices being joined or redirected to a supplementary feature.

Note Logical partitioning policy checks get performed later than digit analysis/calling search space/partition logic during call processing.

The logical partitioning solution comprises the following elements:

- Identifiers—A framework to associate a unique identifier with every device.
- Policies—Allow administrator the ability to define rules or policies that determine the interconnection between any two devices (a VoIP phone and a gateway) in the Cisco Unified Communications Manager system. The configured policies work bidirectionally between the pair of devices.
- Policy Checking—Call processing and features such as transfer, pickup, and ad hoc conference check the defined policies before allowing the calls or features between participants.

Identifiers for Logical Partitioning

Identifiers specify a device type for every device (element) in a Cisco Unified Communications Manager logical partitioning solution. Device types classify all elements into two types: interior and border. Table 21 specifies the Cisco Unified Communications Manager devices that associate with each device type:

Table 21 Device Types and Associated Cisco Unified Communications Manager Devices

Device Type	Cisco Unified Communications Manager Device
Border	Gateway (for example, H.323 Gateway) Intercluster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlled H.225 trunk SIP trunk MGCP port (E1, T1, PRI, BRI, FXO)
Interior	Phones (SCCP, SIP, third party) CTI route points VG224 analog phones MGCP port (FXS) Cisco Unity Voice Mail (SCCP)

Note You cannot edit the classification of Cisco Unified Communications Manager elements: only border and interior designations are allowed, and a particular device can be classified only according to the scheme that Table 21 provides. For example, a SIP trunk can be classified only as a border element.

Allow and Deny Policies for Logical Partitioning

Based on the system requirements for VoIP network topology, you can configure Cisco Unified Communications Manager to provide the following default system policy for logical partitioning:

- Deny—Calls or features get blocked between VoIP device participants of types 1 to 4 (previously enumerated).

  To allow VoIP communication, ensure the Allow policy is configured through logical partitioning configuration.

- Allow—Be aware that calls or features are allowed between VoIP device participants of types 1 to 4 (previously enumerated).

  To deny VoIP communication, ensure the Deny policy is configured through logical partitioning configuration.

Cisco Unified Communications Manager Administration Configuration Tips for Logical Partitioning

Table 22 displays the configuration checklist for logical partitioning, which is documented in the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. Before you configure logical partitioning in your network, review Table 22.

Table 22 Logical Partitioning Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Enable logical partitioning by setting the value of the Enable Logical Partitioning enterprise parameter to **True**.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 2	Define a set of geolocations on a new Geolocation Configuration window.	Geolocation Configuration
Step 3	Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 4	Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.	Geolocation Configuration Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 5	Define the Logical Partitioning Default Policy, which determines whether to allow or deny PSTN calls between devices that associate with valid geolocations and geolocation filters when no explicit Allow/Deny policy is configured in the Logical Partitioning Policy Configuration window for the related geolocation policy records. Use the Enterprise Parameters Configuration window to set the value for the Logical Partitioning Default Policy enterprise parameter.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning

Table 22 Logical Partitioning Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 6	For devices that do not participate in logical partitioning policy checks, define the geolocation as *Unspecified* or leave undefined. **Note** Devices that do not associate with a geolocation or geolocation filter do not participate in logical partitioning policy checks. This lack of association can get defined at the individual-device level, the device-pool level, or the enterprise-parameter level.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 7	Define a set of filter rules in a new Geolocation Filter Configuration window.	Geolocation Filter Configuration
Step 8	Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 9	Assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning
Step 10	Define a set of logical partitioning policy records in a new Logical Partitioning Policy Configuration window.	Logical Partitioning Policy Configuration

Table 22 Logical Partitioning Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 11	Define a set of policies between geolocation policy record device-type pairs: `{{Geolocation Policy1, devType1}, {Geolocation Policy2, devType2}, policyValue}`	Logical Partitioning Policy Configuration
Step 12	To allow devices in different clusters to participate in logical partitioning policy checks, turn on location conveyance as follows: • Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster. • Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.	Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Configuration Checklist for Location Conveyance

See the "Geolocations, Geolocation Filters, and Location Conveyance" section on page 50 for detailed information about the following entities that must be configured for logical partitioning:

- Geolocations
- Geolocation filters

The following entities in a Cisco Unified Communications Manager cluster can have geolocation values assigned:

- Device pools
- CTI route points
- Phones (optional)
- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

Media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, do not need to associate with geolocation values.

Interactions and Limitations for Logical Partitioning

Beyond the configuration of geolocations, geolocation filters, and logical partitioning policies, logical partitioning requires special configuration when an allowed call changes due to the following features:

- Call forwarding
- Call transfer
- Ad hoc conference, Join, Join Across Lines (JAL)
- Meet-me conference
- Call pickup
- Call park and directed call park
- Cisco Extension Mobility
- Cisco Unified Mobility

- Shared line
- Barge, cBarge, and Remote Resume
- Route lists and hunt pilots
- CTI handling

The following limitations apply to logical partitioning:

- SIP trunk User Agent Server (UAS) location conveyance in UPDATE

  The UAS uses UPDATE request to communicate geolocation of the called party to the User Agent Client (UAC). This normally happens after 180 Ringing.

  The logical partitioning policy checks in logical partitioning-aware cluster that receives this geolocation may CANCEL the call if policy gets denied.

- The logical partitioning checks do not get supported for participants across conferences in conference chaining.

  For example, meet-me and ad hoc chained conferences can have participants that have logical partitioning denied.

- Limitation with QSIG intercluster trunk (ICT)

  Be aware that the ICT with Q.SIG protocol is not allowed to communicate geolocation info for the caller or callee device. The ICT configuration for "Send Geolocation Information" gets disabled when the Q.SIG tunneled protocol gets selected.

- Shared Line Active Call Info

  For logical partitioning restricted scenario, the shared line drops the active call information for the duration of the call, even if some feature moves the shared-line call to allowed category.

- cBarge/Barge

  Barge/cBarge does not occur because it gets prevented by not allowing shared lines to attempt these features based on logical partitioning deny policy with the connected party (the call instance gets dropped).

  However, when the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

- Cisco Unified Communications Manager does not communicate geolocation info to H.323 or MGCP gateway.

  Communication to a SIP gateway can get disabled from a SIP trunk check box.

- Cisco Unified Communications Manager does not communicate geolocation information over a H.225 gatekeeper-controlled trunk.

- Scenario: Cisco Unified Communications Manager 1 remains logical partitioning enabled, but Cisco Unified Communications Manager 2 stays logical partitioning disabled.

  Phone A on CCM1 calls Phone B on CCM2 (using ICT or SIP trunk).

  Phone B presses conference and invites PSTN to conference.

  Limitation: The conference gets established.

After phone B goes on hook, the call between phone A and the PSTN on Cisco Unified Communications Manager 2 gets cleared with a reorder tone.

- Mobility Cell Pickup: Logical partitioning Deny handling takes place after call gets answered on the mobile phone.

  The logical partitioning policy check does not happen before the call gets placed to the mobile phone (as it happens for a basic SNR call). The current design checks logical partitioning policy only after SsJoinReq processing, which takes place after the mobile phone answers the call.

- Cisco Extension Mobility logs in to a phone in a different geolocation.

  Outgoing PSTN calls can occur when Local Route Groups are configured.

  Incoming PSTN calls do not get placed to the phone but receive a reorder tone.

- BLF SD or BLF Pickup Presence notifications do not get checked for logical partitioning policy.

  Currently, no logical partitioning infrastructure gets added for notifications.

  For forwarding failures, the RTMT Number of Forwarding Failures performance monitor counter does not increment. Instead, the Number of Basic Call Failures performance monitor counter increments.

- No reorder tone gets provided on IOS H.323 and SIP gateways upon release of connected calls due to logical partitioning policies during supplementary features.

  Example

  Remote destination (RD) phone that is behind IOS SIP or H.323 gateway calls VoIP phone A.

  After authentication completes, RD phone makes a call to phone C, but the call gets denied due to logical partitioning restricted policy.

  Call gets cleared to RD phone with cause 63 (Service or option not available), but no reorder tone gets played to the RD phone.

  Note Be aware that this cause code is common to all logical partitioning failure cases.

  This behavior occurs due to a design limitation on the IOS gateway side, which does not play reorder tone after the CONNECT state. The only tones that play after the CONNECT state specify 17 (Busy) or 44 (No Circuit Available).

  Similar limitations apply for Hook Flash, Onhook Transfer, and other supplementary features.

- No configuration exists for forwarding the call to voice messaging system for logical partitioning failures.
- No announcements occur for logical partitioning deny failures.
- Cisco Unified Communications Manager does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

GUI Changes for Logical Partitioning

Use the following new menu options in Cisco Unified Communications Manager Administration to configure the logical partitioning feature:

- System > Geolocation Configuration
- System > Geolocation Filter
- Call Routing > Logical Partitioning Policy

The following existing Cisco Unified Communications Manager Administration windows contain new fields for configuring logical partitioning:

- Device Pool Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter
- CTI Route Point Configuration—field: Geolocation
- Gateway Configuration—pane: Geolocation Configuration; fields: Geolocation, Geolocation Filter
- Cisco Unified IP Phone Configuration— field: Geolocation
- Trunk Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter, Send Geolocation Information

Service Parameter and Enterprise Parameter Changes for Logical Partitioning

The following new enterprise parameters affect the configuration of the logical partitioning feature:

- Enable Logical Partitioning
- Default Geolocation
- Logical Partitioning Default Policy
- Logical Partitioning Default Filter

Installation/Upgrade (Migration) Considerations for Logical Partitioning

The following migration considerations that affect the dial plan exist for the logical partitioning feature when you are migrating from releases of Cisco Unified Communications Manager earlier than Release 7.1(2):

- If the Enable Logical Partitioning enterprise parameter is set to **True**, geolocations and geolocation filters must get configured for the following entities:
  - Device pools for all phones
  - MGCP ports that access the PSTN
  - H.323 gateways that access the PSTN
  - Intercluster trunks (ICTs, either gatekeeper-controlled or non-gatekeeper-controlled) to remote clusters
  - SIP trunks that access the PSTN or remote clusters
- Ensure that location conveyance is turned on in all clusters to allow end-to-end communication of geolocation information.

  To do so, check the Send Geolocation check box on intercluster trunks (ICTs) and SIP trunks.
- Ensure that logical partitioning policies are configured for all entities for which geolocations and geolocation filters are configured.

During upgrade of Cisco Unified Communications Manager Release 7.1(x) or later from a previous release, the following values get assigned for the entities that associate with logical partitioning configuration:

- Enable Logical Partitioning enterprise parameter specifies **False**.
- Logical Partitioning Default Policy enterprise parameter specifies **Deny**.
- Geolocation
  - No configured geolocation records exist in the geolocation table.
  - Default Geolocation enterprise parameter specifies **Unspecified**.

  - Device pools specify Geolocation value **None**.
  - Devices specify Geolocation value **Default**.
- Geolocation filter
  - No configured geolocation filter records exist in geolocation filter table.
  - Logical Partitioning Default Filter enterprise parameter specifies **None**.
  - Device pools specify Geolocation Filter value **None**.
  - Devices specify Geolocation Filter value **None**.
- Logical partitioning policy
  - No configured GeolocationPolicy records and policies exist in geolocationpolicy and geolocationpolicymatrix tables.

Serviceability Considerations for Logical Partitioning

The following consideration exists for the logical partitioning feature:

- The Cisco Call Restriction counters specify a new group of performance monitoring counters that log the number of failures that result because of logical partitioning policy restrictions. The Cisco Call Restriction counters include the following performance monitoring counters:
  - AdHocConferenceFailures
  - BasicCallFailures
  - ForwardingFailures
  - LogicalPartitionFailuresTotal
  - MeetMeConferenceFailures
  - MidCallFailures
  - ParkRetrievalFailures
  - PickUpFailures
  - SharedLineFailures
  - TransferFailures

  See the “Performance Objects and Counters for Cisco Unified Communications Manager” appendix of the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for details.

BAT Considerations for Logical Partitioning

The Cisco Bulk Administration Tool specifies several new menu items to support logical partitioning. See the “Support for Geolocations and Logical Partitioning” section on page 152 for details.

CAR/CDR Considerations for Logical Partitioning

The following CAR and CDR considerations exist for the logical partitioning feature:

- To support the logical partitioning feature, call termination cause codes get added. See the “Cisco Call Detail Records Codes” chapter of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* for details.
- The “CDR Examples” chapter of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* provides examples of CDRs that are added to support the logical partitioning feature.

Security Considerations for Logical Partitioning

No security considerations exist for the logical partitioning feature.

AXL and CTI Considerations for Logical Partitioning

AXL supports all geolocation-related database changes in Cisco Unified Communications Manager. The AXL SOAP interface gets modified to accommodate all new configuration that the logical partitioning feature requires.

The following CTI considerations exist for the logical partitioning feature:

- CTI handles the new error tags that the logical partitioning feature reports and maps those tags to new CTI error codes.
- When the logical partitioning policy failures result in clearing of the calls, CTI handles the new cause code that gets sent from Cisco Unified Communications Manager, CCM_SIP_503_SERVICE_UNAVAIL_SER_OPTION_NOAVAIL, maps it to the CTI cause code, CtiCcmSip503ServiceNotavailable, and sends it to the application. No new cause code gets added to support the logical partitioning feature.
- For logical partitioning policy failures, the call control sends an SsRedirectCallErr message with a new error code, REDIRECT_CALL_PARTITIONING_POLICY. CTI adds a corresponding CTI error code for these SsRedirectCallErr messages.

User Tips for Logical Partitioning

No user tips exist for the logical partitioning feature.

For More Information About Logical Partitioning

- Logical Partitioning, *Cisco Unified Communications Manager Features and Services Guide*
- Geolocations and Location Conveyance, *Cisco Unified Communications Manager Features and Services Guide*
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*
- CTI Route Point Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Performance Objects and Counters for Cisco Unified Communications Manager, *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- Cisco Call Details Records Codes, *Cisco Unified Communications Manager Call Detail Records Administration Guide*
- CDR Examples, *Cisco Unified Communications Manager Call Detail Records Administration Guide*
- *Cisco Unified Reporting Administration Guide*

Multicast Music On Hold Over H.323 Intercluster Trunks

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

The Multicast Music on Hold (MOH) over H.323 Trunk feature allows multicast MOH to work over H.323 intercluster trunks (ICTs). Prior to the implementation of this feature, multicast MOH used bandwidth for each unicast MOH over the same ICT, which wasted bandwidth.

Prior to the implementation of this feature in 6.1(3) and 7.1(2), the H.323 Open Logical Channel (OLC) ACK message carried the IP address and port for multicast MOH. With the implementation of this feature, the H.323 OLC message now carries the IP address and port for multicast MOH, and Cisco Unified Communications Manager adds the mechanism to handle the information in the H.323 OLC message.

The new service parameter, Send Multicast MOH in H.245 OLC Message, controls the Multicast Music On Hold Over H.323 Intercluster Trunk feature. Both Cisco Unified Communications Manager nodes that are involved in the call must support single-transmitter multicast for the setting of this parameter to have any effect. This service parameter affects only the side of the party that places the call on hold and does not affect how the far end carries the multicast transport address. Even if this parameter is turned off, multicast MOH applies for the held-party side of the call as long as the held party has the capability to support single-transmitter multicast.

When a call connects over an intercluster trunk and one of the parties presses the Hold key, MOH will stream over the intercluster trunk. If multicast MOH is turned on and the holding party and trunk are configured to use the multicast MOH server, MOH streams with multicast. Only one multicast MOH stream streams over the trunk no matter how many calls are put on hold on this trunk.

Cisco Unified Communications Manager Administration Configuration Tips

Calls that connect over Cisco Unified Communications Manager intercluster trunks use this feature for multicast MOH. This feature does not work if any middle box between Cisco Unified Communications Managers does not pass the new fields in Terminal Capability Set (TCS) and OLC message.

No additional configuration exists for this new feature in addition to the normal configuration for setting up multicast MOH. This new feature only applies between Cisco Unified Communications Managers that support single-transmitter multicast.

You can turn this feature off by changing the default True value of the new Send Multicast MOH in H.245 OLC Message service parameter to False. You may need to do so if an interoperability issue arises.

GUI Changes

This feature does not entail any GUI changes to Cisco Unified Communications Manager Administration.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Send Multicast MOH in H.245 OLC Message, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Send Multicast OH in H.245 OLC Message drop-down list box, choose **True**.

The new feature stays active by default. To turn off the feature, set the value of the Send Multicast MOH in H.245 OLC Message service parameter to **False**. Do so to resolve interoperability issues that the feature may cause.

The new service parameter governs the multicast MOH behavior on H.323 trunks and devices. The new service parameter does not control multicast MOH over SIP trunks because multicast MOH over SIP trunks does not constitute a new behavior.

Installation/Upgrade (Migration) Considerations

No installation nor upgrade considerations exist for this feature. You may, however, turn off the feature if interoperability issues arise as a result of the feature. To do so, set the value of the Send Multicast MOH in H.245 OLC Message service parameter to **False**.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL considerations exist for this feature.

CTI-controlled phones work as before for multicast MOH. CTI-controlled applications such as CTI ports and CTI route points do not perform multicast MOH, which is the same behavior as prior to the implementation of this feature.

User Tips

When multicast MOH gets turned on in Cisco Unified Communications Manager Administration, phone users receive MOH if the call connects through an intercluster trunk.

For More Information

- Music on Hold, *Cisco Unified Communications Manager Features and Services Guide*

Off-Hook Abbreviated Dial

Description

Cisco Unified Communications Manager Release 7.1(2) introduces an enhancement to the existing Abbreviated Dial feature to allow abbreviated dialing while off hook. The user can initiate Off-Hook Abbreviated Dialing while placing a basic call, while conferencing a call, while transferring a call, or while a call is on hold.

To enable Off-Hook Abbreviated Dialing, assign the softkey Abbreviated Dial (AbbrDial) to a softkey template and assign the template to the phone. Be aware that the Abbreviated Dial (AbbrDial) softkey can be included in the Off Hook, Off Hook With Feature, or Digits After First states of a Softkey Layout Configuration.

Cisco Unified Communications Manager Administration Configuration Tips

Step 1 Find the softkey template:

a. Choose **Device > Device Settings > Softkey Template.**

The Find and List Softkey Templates window displays. Records from an active (prior) query may also display in the window.

b. To find all records in the database, ensure the dialog box is empty; go to sub-step c.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.
- From the third drop-down list box, select whether to search for standard, non-standard, or both types of softkey templates.

c. Click **Find**.

All matching records display.

Step 2 Add the Abbreviated Dial (AbbrDial) softkey to the off-hook call states:

a. From the list of matching records, choose the softkey template in which you want to configure softkey positions. The Softkey Template Configuration window displays.

Note You can modify only softkey templates that display a check box in the left column. All other softkey templates comprise standard, read-only templates.

b. Choose **Configure Softkey Layout** from the Related Links drop-down list box; then, click **Go**.

The Softkey Layout Configuration window displays. The Select a call state to configure drop-down list box lists each Cisco Unified Communications Manager call state for an IP phone.

c. Change the off-hook call states to include the Abbreviated Dial (AbbrDial) softkey. The off-hook call states include Off Hook, Off Hook With Feature, and Digits After First. You must add the Abbreviated Dial (AbbrDial) softkey to each of these call states.

- From the Select a call state to configure drop-down list box, select Off-hook. The Softkey Layout Configuration window redisplays, and the Unselected Softkeys pane and Selected Softkeys pane display the softkeys that are applicable to the call state.
- Move the Abbreviated Dial (AbbrDial) softkey to the Selected Softkeys list by using the arrows between the panes.
- To rearrange the positions of the Selected Softkeys, use the up and down arrows to the right of the Selected Softkeys pane.
- To save your softkey layout configuration, click **Save**.
- Repeat these steps for the call states Off Hook With Feature and Digits After First. You must add the Abbreviated Dial (AbbrDial) softkey to all three off-hook call states, including Off Hook, Off Hook With Feature, and Digits After First.

d. To return to the Softkey Template Configuration window, choose the Softkey Template Configuration link from the Related Links drop-down list box in the upper, right corner; then, click **Go**.

e. To save your configuration, click **Save**.

f. To make the updates of the softkey template take effect on the phone, click **Reset**. To assign a template to a phone, see "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide.*

GUI Changes

No GUI changes occurred to support this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes occurred to support this feature.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 7.1(2) introduces this feature. After you install or upgrade to 7.1(2), you can configure this feature.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that you activated the Cisco CallManager service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration Tool (BAT) supports the import and export of the AbbrDial softkey configuration.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For information on user tips and phone support for this feature, see "Off-Hook Abbreviated Dialing" section on page 190.

For More Information

- "Softkey Template Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*

OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database

DirSync allows you to synchronize the data from corporate directories to Cisco Unified Communications Manager. Cisco Unified Communications Manager Release 7.1(2) allows synchronization from OpenLDAP 2.3.41 to the Cisco Unified Communications Manager database. In addition, Cisco Unified Communications Manager Release 7.1(2) 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*.

Party Entrance Tone

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

Tip To configure the party entrance tone in previous releases of Cisco Unified Communications Manager [except for 6.1(3)], you configured the party entrance tone service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(2) and 6.1(3), you can configure the party entrance tone for directory numbers on a phone.

With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multiparty call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call.

If the controlling device, that is, the originator of the multiparty call has a built-in bridge, the tone plays to all parties if you configured party tone entrance for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.

When a joined call or ad hoc conference begins, Cisco Unified Communications Manager uses the party entrance tone configuration from the conference controller. Cisco Unified Communications Manager uses this configuration until the conference ends.

If two ad hoc conferences are chained together and the controlling device for one conference has the party entrance tone set to True while the other controlling device for the other conference has a party entrance tone of False, Cisco Unified Communications Manager determines whether to play the tone based on to which conference the new party is added.

When a barge call gets created, the party entrance tone configuration of the barge target that shares the line with the barge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone.

When a cBarge call gets created, the party entrance tone configuration of the cBarge target that shares the line with the cBarge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone. However, if the call for the target is an existing ad hoc conference that is in the same cluster, the party entrance tone configuration for the ad hoc conference controller determines whether Cisco Unified Communications Manager plays the tone.

When a meet-me conference gets created, the party entrance tone configuration for the first party to enter the conference determines whether Cisco Unified Communications Manager plays the tone. Cisco Unified Communications Manager uses the configuration for the first party until the conference ends.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure that the controlling device for the multiparty call has a built-in bridge.

To configure the party entrance tone for a specific directory number, choose **Call Routing > Directory Number** in Cisco Unified Communications Manager Administration. From the Party Entrance Tone drop-down list box, choose one of the following options:

- **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
- **On**—A tone plays on the phone when a basic call changes to a multiparty call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call. If the controlling device, that is, the originator of the multiparty call, has a built-in bridge, the tone plays to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.
- **Off**—A tone does not play on the phone when a basic call changes to a multiparty call.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature for the entire cluster instead of per line, configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service. To access this parameter, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration; choose the server and the **Cisco CallManager** service. When the parameters display, locate the Party Entrance Tone service parameter. For more information on this parameter, click the name of the service parameter or the question-mark button in the Service Parameter Configuration window.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 7.1(2) introduces this feature.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that the service is activated in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration GUI has the following updates to support the party entrance tone feature:

- Party Entrance Tone drop-down list box—Choose one of the following options:
  - **Default**—Use the value that you configured in the Party Entrance Tone service parameter.

  - **On**—A tone plays on the phone when a basic call changes to a multiparty call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call. If the controlling device, that is, the originator of the multiparty call, has a built-in bridge, the tone plays to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.
  - **Off**—A tone does not play on the phone when a basic call changes to a multiparty call.

Note The Party Entrance Tone drop-down list box displays in the Phone Line Template, UDP Line Template, UDP Update Line, RDP Line Template, Phone Update Line, and UDP Update Line windows.

- Insert, Export, and Validate Details support for party entrance tone—The following insert, export, and validate details features include support for the party entrance tone:
  - 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
  - Insert Gateways
  - Insert Remote Destination Profiles
  - Export Remote Destination Profiles
- File Formats—The following file formats support the party entrance tone feature:
  - Phone File Format—Party Entrance Tone field displays as a part of the Line Fields section.
  - UDP File Format—Party Entrance Tone field displays as a part of the Line Fields section.
  - Remote Destination Profile File Format—Party Entrance Tone field displays as a part of the Line Fields section.

Note For more information on BAT, refer to the Bulk Administration Tool section of this document.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "Barge Enhancement Feature" section on page 182.

User Tips

For information on the phones that support this feature, see the "Barge Tone Enhancements" section on page 185.

For More Information

- Barge Tone Enhancements, page 185

Phone Migration in Cisco Unified Communications Manager Administration

Description

The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone; that is, you can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, or you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP), and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

Tip Phone migration allows you to port existing phone configuration to a new phone without needing to add a phone, lines, speed dials, and so on.

Cisco Unified Communications Manager Administration Configuration Tips

Before you can migrate phone configuration to a new phone, consider the following information:

- If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.
- Some phone models do not support phone migration; for example, CTI port and H.323 client, Cisco Unified Mobile Communicator.
- Before you can migrate the phone configuration in Cisco Unified Communications Manager Administration, you must create a phone template for the phone model to which you want to migrate in BAT (Bulk Administration > Phones > Phone Template). For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.
- The new phone uses the same PKID and existing phone record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration.

Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some of the speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.

- Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network.
- Before you migrate the phone configuration to a new phone, ensure that you have the appropriate device licenses for the new phone.

GUI Changes

Table 23 describes the configuration settings that display in the Phone Migration Configuration window.

Table 23 Phone Migration Configuration Settings

Field	Description
Phone Template	From the drop-down list box, choose the phone template for the phone model to which you want to migrate the phone configuration. Only the phone templates that you configured in the Phone Template window in Bulk Administration display (Bulk Administration > Phones > Phone Template).
MAC Address	Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.
Description	If you want to do so, enter a description for the new phone.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(2), you can use this feature.

Serviceability Considerations

No special serviceability considerations exist for this feature.

BAT Considerations

Before you can migrate the phone configuration in Cisco Unified Communications Manager Administration, you must create a phone template for the phone model to which you want to migrate in BAT (Bulk Administration > Phones > Phone Template). For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.

If you want to migrate several phones at the same time, consider using BAT, as described in the "Phone Migration in BAT" section on page 150.

CAR/CDR Considerations

No CDR or CAR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

User Tips

No end user tips exist for this feature.

For More Information

- Phone Migration in BAT, page 150

QSIG Variant Configuration for a Gateway or Trunk

Description

The QSIG variant specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations, as well as how to code the protocol profile for outbound facility Information elements.

Cisco Unified Communications Manager Release 7.1(2) introduces an enhancement to the existing QSIG variant feature to allow CCM administrators to configure QSIG variants for s specific trunk or gateway. In previous releases, you could configure the QSIG variant for cluster service configurations only.

Cisco Unified Communications Manager Release 7.1(2) also introduces support by using Annex M.1 to tunnel QSIG over intercluster trunks with the QSIG Variant ECMA.

Cisco Unified Communications Manager Administration Configuration Tips

To create Cisco Unified Communications Manager compatibility with your version of the QSIG protocol, configure the ASN.1 ROSE OID Encoding and QSIG Variant in the service parameters, for a gateway, or for a trunk.

Tip For more information on these parameters, click the **?** that displays in the upper corner of the Service Parameter window.

If you choose ECMA for the QSIG Variant parameter, you must choose the Use Global Value (ECMA) setting for the ASN.1 ROSE OID Encoding service parameter.

If you choose ISO for the QSIG Variant parameter, you normally choose the Use Local Value setting for the ASN.1 ROSE OID Encoding service parameter. You may need other configurations in unusual situations.

Tip To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. Keep the QSIG Variant and ASN.1 ROSE OID Encoding parameters set to the default value unless a Cisco support engineer instructs otherwise.

Cisco Unified Communications Manager supports using Annex M.1 to tunnel QSIG over intercluster trunks. To configure Annex M.1, do one of the following tasks:

- Set the ASN.1 ROSE OID Encoding to Use Local Value and the QSIG Variant to ISO (Protocol Profile 0x9F).

- Set the ASN.1 ROSE OID Encoding to Use Global Value (ECMA) and the QSIG Variant to ECMA.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that you activated the Cisco CallManager service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration Tool (BAT) supports the import and export of the QSIG variant configuration.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "QSIG variant Per Trunk or Gateway" section on page 181.

User Tips

This feature update does not impact end users.

For More Information

- "Gateway Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Trunk Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Service Parameters Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Understanding IP Telephony Protocols," *Cisco Unified Communications Manager System Guide*

Standard Audit Log Administration Role

The Standard Audit Log role allows you to configure the following Resource Access Information. For each item, you can choose Read access, Update access, or both.

- Alarm Configuration window
- Alarm Definition window
- Audit Configuration
- Audit Trace
- CDR Management
- Control Center - Feature Services window
- Control Center - Network Services window
- Log Partition Monitoring->Configuration window
- RTMT->Alert Config
- RTMT->Profile Saving
- Real Time Monitoring Tool
- SNMP->V1/V2c->Configuration->Community String window

- SNMP->V1/V2c->Configuration->Notification Destination window
- SNMP->V3 Configuration->Notification Destination window
- SNMP->V3 Configuration->User window
- SNMP->system Group Configuration->MIB2 System Group Configuration window
- SOAP Backup and Restore APIs
- SOAP CDR on Demand APIs
- SOAP Control Center APIs
- SOAP Log Collection APIs
- SOAP Performance Informations APIs
- SOAP Realtime Informations and Control Center APIs
- SOAP SNMP Config API
- Service Activation window
- Serviceability Report Archive
- Trace Collection Tool
- Trace Configuration window
- Troubleshoot Trace Settings window

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(2) or upgrade to 7.1(2), you can use this feature.

Serviceability Considerations

For more information, refer to the "Audit Logging" section on page 155.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

Standard Audit Users User Group

Only a user or application that is assigned to the Standard Audit Users user group can change audit log settings. By default, the CCMAdministrator application user gets assigned to the Standard Audit Users user group and can add or delete users from the Standard Audit Users user group.

You can configure the audit log settings that can be changed by a Standard Audit Log user through the Standard Audit Log Administration role. See the "Standard Audit Log Administration Role" section on page 131.

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(2) or upgrade to 7.1(2), you can use this feature.

Serviceability Considerations

For more information, refer to the "Audit Logging" section on page 155.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

Synchronization of Configuration Settings

Description

Cisco Unified Communications Manager Release 7.1(2) allows you to use a single button in Cisco Unified Communications Manager Administration to synchronize various devices with the most recent configuration changes. This button gets called "Apply Config" when it is located on a configuration window and gets called "Apply Config to Selected" when it is located in a Find and List window. These buttons apply any outstanding configuration settings in the least-intrusive manner possible. (For example, some devices may not require a reset/restart to apply the configuration.)

Cisco Unified Communications Manager Administration Configuration Tips

To synchronize a device with the most recent configuration changes, perform the following procedure.

Procedure

Step 1 Navigate to one of the windows that are listed in Table 24. Table 24 lists all the windows in Cisco Unified Communications Manager Administration, organized by menu, that provide the configuration synchronization function.

The Find and List window for the applicable items displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.

Step 4 The window displays a list of items that match the search criteria.

a. If the window shows a button that is called **Apply Config to Selected**, perform the following tasks (otherwise, proceed to b.):

- Check the check boxes next to the items that you want to synchronize. To choose all items in the window, check the check box in the matching records title bar.
- Click **Apply Config to Selected.**
- Proceed to Step 5.

b. If the window *does not* show a button that is called **Apply Config to Selected**, perform the following tasks:

- Click the item that you want to synchronize.
- The configuration window for the item that you clicked displays.

  Make any additional configuration changes.

  Click **Save**.

  Click **Apply Config**.

  Proceed to Step 5.

Step 5 The **Apply Configuration Information** dialog displays.

Note The device(s) may need to restart for configuration changes to take effect.

Click **OK**.

Table 24 Windows for Synchronizing Configuration Settings

Navigation Path to Window	Window Name
System Menu	
System > Cisco Unified CM	Cisco Unified CM Configuration
System > Cisco Unified CM Group	Cisco Unified CM Group Configuration
System > Date/Time Group	Date/Time Group Configuration
System > Region	Region Configuration
System > Device Pool	Device Pool Configuration
System > Enterprise Parameters	Enterprise Parameters Configuration
System > Security > Phone Security Profile	Phone Security Profile Configuration

Table 24 Windows for Synchronizing Configuration Settings (continued)

Navigation Path to Window	Window Name
System > Security > SIP Trunk Security Profile	SIP Trunk Security Profile Configuration
Call Routing Menu	
Call Routing > Dial Rules > SIP Dial Rules	SIP Dial Rule Configuration
Call Routing > Route Filter	Route Filter Configuration
Call Routing > Route Hunt > Route List	Find and List Route Lists
Call Routing > Route Hunt > Hunt List	Find and List Hunt Lists
Call Routing > Class of Control > Partition	Partition Configuration
Call Routing > Intercom > Intercom Route Partition	Intercom Partition Configuration
Call Routing > Intercom > Intercom Directory Number	Intercom Directory Number Configuration
Call Routing > Directed Call Park	Directed Call Park Configuration
Call Routing > Directory Number	Directory Number Configuration
Media Resources Menu	
Media Resources > Annunciator	Find and List Annunciators
Media Resources > Conference Bridge	Find and List Conference Bridges
Media Resources > Media Termination Point	Find and List Media Termination Points
Media Resources > Music On Hold Server	Find and List Music On Hold Servers
Media Resources > Transcoder	Find and List Transcoders
Voice Mail Menu	
Voice Mail > Cisco Voice Mail Port	Find and List Cisco Voice Mail Ports
Voice Mail > Voice Mail Profile	Voice Mail Profile Configuration
Device Menu	
Device > CTI Route Point	Find and List CTI Route Points
Device > Gatekeeper	CTI Route Point Gatekeepers
Device > Gateway	Find and List Gateway
Device > Phone	Find and List Phones
Device > Trunk	Find and List Trunks
Device > Device Settings > Softkey Template	Softkey Template Configuration
Device > Device Settings > SIP Profile	SIP Profile Configuration
Device > Device Settings > Common Device Configuration	Common Device Configuration
Device > Device Settings > Common Phone Profile	Common Phone Profile Configuration
Application Menu	
Application > Cisco Unified CM Attendant Console > Pilot Point	Find and List Pilot Points

GUI Changes

Cisco Unified Communications Manager Administration added the "Apply Config" or "Apply Config to Selected" buttons to the windows that are listed in Table 24.

Service Parameter and Enterprise Parameter Changes

The Enterprise Parameters Configuration window (**System > Enterprise Parameters**) contains the “Apply Config” button.

Installation/Upgrade (Migration) Considerations

No specific installation or upgrade considerations exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

BAT supports this feature by enabling the “Apply Config” button in the following windows:

- Bulk Administration > Phones > Update Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.
- Bulk Administration > Phones > Reset/Restart Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

For More Information

Refer to configuration information as it pertains to the windows that are listed in Table 24 in the following documents:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager System Guide*

Table Out of Sync Detection

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

When the Table Out Of Sync parameter is turned on, the Database Replication Status summary gets collected every day during the maintenance window. The system compares the output of three consecutive days to determine whether tables have been out of sync for all three days. If so, it triggers an alert.

This parameter, by default, gets set to Off and runs at the time that is specified in Maintenance Time parameter.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

To use the database table out of sync feature, ensure that you turn the parameter on.

To enable the database table out of sync feature, perform the following procedure:

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Service Parameter.**

Step 2 From the Server drop-down list, select the server.

Step 3 From the Service drop-down list, select **Cisco Database Layer Monitor.**

Step 4 Set the Maintenance Time parameter value.

Step 5 Set the Maintenance Window parameter value.

Step 6 From the Table Out of Sync Detection drop-down list, choose **On**.

Step 7 From the MaintenanceTaskTrace drop-down list, choose **On**.

Step 8 Click **Save**.

Steps to Ensure That You are Notified of Inconsistencies

To ensure that you will be notified if the databases on the publisher server and the subscriber servers are inconsistent, you should perform the following tasks:

- Complete the steps that are described in "Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes" section on page 137.
- Enable the alert.
- Configure the Alert in RTMT.

Enable the Alert

To enable Cisco Unified CM to alert you in case of out of sync conditions, perform the following steps from Cisco Unified Serviceability:

Step 1 From the Alarm menu, choose **Configuration**.

Step 2 From the server drop-down list, choose your server.

Step 3 From from the Service Group drop-down list, choose **Database and Admin Services** and click **Go**.

Step 4 From the Service drop-down list, choose **Cisco Database Monitor Layer Monitor** and click **Go**.

Step 5 In the SDI Trace field, click **Enable Alarm** and set the Alarm Event Level to.....

Step 6 Click **Save**.

Configure the Alert in RTMT

To configure the alert in RTMT, see the Setting Alert Properties information in the *Cisco Unified Real-time Monitoring Tool Guide*.

Note You can configure RTMT to make you aware of this alarm via e-mail.

Note Cisco recommends that you call TAC if this alert gets generated.

For More Information

- *Cisco Unified Real-time Monitoring Tool Guide*

Unconfigured Device Registration Attempts Restricted

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Prior to Cisco Unified Communications Manager 6.1(3) or 7.1(2) (not 7.0(1), if a Cisco Unified IP Phone had not been added to the Cisco Unified Communications Manager database and did not have auto-registration enabled, the phone would repeatedly attempt to register (unsuccessfully) with Cisco Unified Communications Manager, thus wasting Cisco Unified Communications Manager capacity with these repeated registration requests.

However, in Cisco Unified Communications Manager 6.1(3) or 7.1(2), if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone will not attempt to register with Cisco Unified Communications Manager. The phone continues to display the Configuring IP message until auto-registration gets enabled or until the phone gets added to the Cisco Unified Communications Manager database.

Supported Devices

The following devices support this changed registration behavior:

- IP Phone 7906G
- IP Phone 7911G
- IP Phone 7931G
- IP Phone 7941G
- IP Phone 7942G
- IP Phone 7945G
- IP Phone 7961G
- IP Phone 7962G
- IP Phone 7965G
- IP Phone 7970G
- IP Phone 7971G
- IP Phone 7975G
- Cisco Analog Telephone Adapter
- VG248 Gateways

Cisco Unified Communications Manager Administration Configuration Tips

For information on configuring autoregistration, refer to the "Autoregistration" chapter in the *Cisco Unified Communications Manager System Guide*. For information on configuring a phone, refer to the "Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Before you configure a phone, consider the following information:

- If the Cisco Unified Communications Manager database contains a real MAC address for a phone, not the dummy MAC address that is created via the Bulk Administration Tool (BAT), licensing immediately consumes device license units for the phone after the phone gets added to the database.
  - If the number of used device license units and number of pending device licensing units do not exceed the total number of device license units that are available for use, the phone with the real MAC address gets added to the database.
  - If the number of used device license units and number of pending device licensing units exceed the total number of device license units that are available for use, the phone with the real MAC address does not get added to the database.
- Licensing uses the Is Active check box in the Phone Configuration window in Cisco Unified Communications Manager Administration to determine whether to consume device license units for the phone. In addition, Cisco Unified Communications Manager uses this check box to determine whether a phone should register with Cisco Unified Communications Manager.

  For a phone that uses a real MAC address, not the dummy MAC address that is created via BAT, the check box displays as checked and disabled, which indicates that the phone uses device license units and can register with Cisco Unified Communications Manager.

  For a phone that uses the dummy MAC address that is created via BAT, the Is Active check box displays as unchecked and enabled. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, check the Is Active check box, which ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone.
- Cisco Unified Communications Manager allows you to provision phones with dummy MAC addresses via BAT as long as the number of used device license units and the number of pending device license units do not exceed the total number of device license units that are available for use.
- If you use the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS) to associate an auto-registered phone with the BAT dummy settings, the Cisco Unified Communications Manager Auto-Register Phone Tool deletes the auto-registered phone from the database, and licensing gives you credits for the device license units for the deleted phone. After the Cisco Unified Communications Manager Auto-Register Phone Tool applies the device name to the phone that uses the dummy MAC address, the Cisco Unified Communications Manager Auto-Register Phone Tool updates the Is Active check box to display as checked and disabled. Licensing consumes device license units for the phone, and the phone can register with Cisco Unified Communications Manager, unless the number of used device license units exceeds the total number of device license units that are available for use.
- When a phone auto-registers for use with the Cisco Unified Communications Manager Auto-Register Phone Tool, it gets inserted into the database as long as the number of used device license units is less than the number of device license units that are available for use.
- You can view the number of pending, used, and available device license units in the License Unit Report and the License Unit Calculator in Cisco Unified Communications Manager Administration.

GUI Changes

No new fields display in Cisco Unified Communications Manager Administration for this feature.

Service Parameter and Enterprise Parameter Changes

No parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(2), if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager.

Serviceability Considerations

The Cisco Unified Real-Time Monitoring Tool and Cisco Unified Reporting can display information on registered and unregistered devices. For more information, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* and the *Cisco Unified Reporting Administration Guide*.

BAT Considerations

For information on adding devices through BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

If the Configuring IP message displays on the phone, the phone user should contact the phone administrator.

Viewing Held Calls on Shared Lines

Tip Cisco Unified Communications Manager Releases 7.1(2) and 6.1(3) introduce this feature.

Description

With the held calls on shared lines feature, a phone user can determine whether the call was put on hold by the phone user locally at the primary device or by another party remotely on a shared device. How the held call displays on the devices depends on whether the primary device or shared device puts the call on hold. For information on how the held call displays on the devices, see the "Hold Status" section on page 186.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

This feature requires no configuration in Cisco Unified Communications Manager Administration to work. This feature works automatically after you install Cisco Unified Communications Manager 6.1(3) or 7.1(2).

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration in Cisco Unified Communications Manager Administration to work. This feature works automatically after you install Cisco Unified Communications Manager 6.1(3) or 7.1(2).

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(2) or upgrade to 7.1(2), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Hold Status" section on page 186.

For More Information

- Hold Status, page 186

Security

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

- CAPF Interaction with IPv6 Addressing, page 141
- SSH Credentials in the Common Device Profile window, page 143
- H.235 Pass-Through Support, page 143
- CTL File Size Limitation, page 144
- Security Icons, page 144
- Cisco Security Agent Version, page 146
- Accessing Cisco Security Agent Logs, page 146

CAPF Interaction with IPv6 Addressing

Description

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. To secure phones with IPv6 or IPv4 addresses, you must use CAPF. Table 25 describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 25 How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv6	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv4	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6	IPv6	IPv4	Phone cannot connect to CAPF.

Cisco Unified Communications Manager Administration Configuration Tips

To issue or upgrade certificates for phones that are running SCCP that use an IPv6 address, you must set the Enable IPv6 service parameter to **True** in Cisco Unified Communications Manager Administration.

For More Information

- Internet Protocol Version 6 (IPv6), page 64
- *Cisco Unified Communications Manager Security Guide*

SSH Credentials in the Common Device Profile window

Prior to Release 7.1(2), the SSH credentials fields only displayed in the Device Profile window for individual devices. The SSH credentials fields now also display in the Common Device Profile window, so you can set them as part of the common device profile.

For information on AXL support, see the "SSH Userid and Password Configured in the Common Phone Profile" section on page 183.

H.235 Pass-Through Support

Description

Cisco Unified Communications Manager allows some types of gateways and trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To enable the passing through of H.235 data, check the **H.235 pass through allowed** check box in the configuration settings of the following trunks and gateways:

- H.225 Trunk
- ICT Gatekeeper Control
- ICT non-Gatekeeper Control
- H.323 Gateway

Cisco Unified Communications Manager Administration Configuration Tips

No configuration tips exist for this feature.

GUI Changes

The **H.235 pass through allowed** check box displays in the configuration window for each type of trunk and gateway that supports H.235 pass-through.

Service Parameter and Enterprise Parameter Changes

No service parameter or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade considerations exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

Some types of gateways and trunks can transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

AXL and CTI Considerations

See the "H.323 Security: Voice Encryption Profile with Native H.235/H.245 Key Management" section on page 180.

User Tips

No user tips exist.

For More Information

- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Administration Guide*

CTL File Size Limitation

The Cisco CTL Client limits the file size of a CTL file to 32 kilobytes because the phones cannot accept a larger CTL file. The following factors affect the size of a CTL file:

- The number of nodes in the cluster
- More nodes that require more certificates in the CTL file
- The number of firewalls that are used for TLS Proxy

  Firewalls with TLS Proxy feature act the same as nodes and therefore get included in the CTL file.
- Whether an external certificate authority (CA) is used to sign the CAPF and CallManager certificates

  Because certificates (CAPF/CallManager) that are signed by an external CA are significantly larger than default self-signed certificates, this can limit the maximum number of certificates that can fit into the CTL file.

These factors directly limit the maximum number of certificates that you can fit in a 32-kilobyte CTL file, and therefore they dictate the maximum number of nodes or firewalls that you can have in a secure Cisco Unified Communications Manager deployment.

Security Icons

Description

Cisco Unified Communications Manager provides security status for a call, according to security levels that are configured for the Cisco Unified Communications Manager server(s) and devices that are participating in the call.

Phones that support security icons display the call security level.

- The phone displays a shield icon for calls with a signaling security level of authenticated. A shield identifies a secured connection between Cisco IP devices, which means that the devices have authenticated or encrypted signaling.
- The phone displays a lock icon for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.

Note Some phone models display only the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints. If a SIP trunk is involved in a call path, the call session status specifies nonsecure. Refer to *Cisco Unified Communications Manager Security Guide* for restrictions that are associated with security icons.

The call gets considered as secure only if both the audio and video portions are secure. Table 26 describes the rules that determine whether a security icon displays and which icon displays.

Table 26 Security Icon Display Rules

Media and Device Types In the Call	Phones That Display Both Shield and Lock Icons	Phones That Display Only the Lock Icon
Secure audio only	Lock	Lock
Secure audio with unsecure video	Shield	None
Secure audio with secure video	Lock	Lock
Authenticated device with nonsecure audio only	Shield	None
Authenticated device with nonsecure audio and video	Shield	None
Unauthenticated device with nonsecure audio only	None	None
Unauthenticated device with nonsecure audio and video	None	None

For conference and barge calls, the security icon displays the security status for the conference.

Cisco Unified Communications Manager Administration Configuration Tips

This feature requires no configuration to work.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service parameter or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade considerations exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

This feature changes the rules that determine the display of secure icons on secure phones.

AXL and CTI Considerations

No AXL considerations exist for this feature.

User Tips

None

For More Information

- *Cisco Unified Communications Manager Security Guide*

Cisco Security Agent Version

This release of Cisco Unified Communications Manager includes Cisco Security Agent version 5.2.

Accessing Cisco Security Agent Logs

The CLI command that accesses the log for Cisco Security Agent gets changed to **utils create report csa**. Refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions* for more information about starting a CLI session and using CLI commands.

Bulk Administration Tool

This section contains information on the following topics:

- Support for Party Entrance Tone, page 146
- Support for Log Missed Calls, page 148
- Support for Always Use Prime Line, page 149
- Support for VG202 and VG204 Gateways, page 150
- Phone Migration in BAT, page 150
- Support for Geolocations and Logical Partitioning, page 152
- New fields That Are Supported for Export by Import/Export, page 152
- Support for Seamless Integration (Apply Config), page 152

Support for Party Entrance Tone

The Bulk Administration GUI includes the following updates to support the party entrance tone feature:

- Party Entrance Tone drop-down list box—Choose one of the following options:
  - **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
  - **On**—A tone plays on the phone when a basic call changes to a multiparty call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call. If the controlling device, that is, the originator of the multiparty call has a built-in bridge, the tone plays to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified

Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.

- **Off**—A tone does not play on the phone when a basic call changes to a multiparty call.

Note The Party Entrance Tone drop-down list box displays in the Phone Line Template, UDP Line Template, gateway Line Template, UDP Update Line, RDP Line Template, and Phone Update Line windows.

- Insert, Export, and Validate Details support for party entrance tone—The following insert, export, and validate details features include support for the party entrance tone:
  - 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
  - Insert Gateways
  - Insert Remote Destination Profiles
  - Export Remote Destination Profiles
  - Phone Add lines
  - UDP Add Lines
  - Phone Update Lines
  - UDP Update Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—The following file formats support the party entrance tone feature:
  - Phone File Format—Party Entrance Tone field comprises a part of the Line Fields section.
  - UDP File Format—Party Entrance Tone field comprises a part of the Line Fields section.
  - Remote Destination Profile File Format—Party Entrance Tone field is a part of the Line Fields section.

- Generate Phone Report—The Generate Phone Report Configuration window lists the Party Entrance Tone field in the Line Fields section.

Support for Log Missed Calls

The Bulk Administration GUI includes the following updates to support the Log Missed Calls feature:

- Log Missed Calls Check Box— This check box allows you to turn this feature on or off. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone.

Note The Log Missed Calls Check Box displays in the Phone Line Template, UDP Line Template, Phone Update Line, and UDP Update Line windows.

- Insert, Export, and Validate Details support for the log missed calls feature—The following insert, export, and validate details features include support for the log missed calls feature:
  - 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
  - Phone Add lines
  - UDP Add Lines
  - Phone Update Lines
  - UDP Update Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—The following file formats support the missed logged calls feature:
  - Phone File Format—Missed logged calls field comprise a part of the Line Fields section.
  - UDP File Format—Missed logged calls field comprise a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Log Missed Calls field in the Line Fields section.

- Generate Phone Report—The Generate Phone Report Configuration window lists the Log Missed Calls field in the Line Fields section.

Support for Always Use Prime Line

The Bulk Administration GUI includes the following updates to support the Always Use Prime Line feature:

- Always Use Prime Line drop-down list box—Choose one of the following options:
  - Off
  - On
  - Default
- Always Use Prime Line for Voice Message drop-down list box—Choose one of the following options:
  - Off
  - On
  - Default

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 3 and Table 4.

Note The Always Use Prime Line and Always Use Prime Line for Voice Message drop-down list boxes display in the Phone Template, UDP Template, and Update Phone windows.

- Insert, Export, and Validate Details support for always use prime line—The following insert, export, and validate details features include support for the always use prime line feature:
  - 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

- Phone File Format—Phone File Format Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- UDP File Format—UDP File Format Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Fields section.
- Generate Phone Report—The Generate Phone Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Line Fields section.

Support for VG202 and VG204 Gateways

BAT now supports VG202 and VG204 gateways. The Bulk Administration Tool includes the following updates to support VG202 and VG204 gateways:

- Bulk Administration > Gateways > Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration > Gateways > Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration > Gateways > Insert Gateways. Select Gateway type as VG202 or VG204 and click Next. The second Insert Gateways Configuration window displays—The View Sample File link displays VG202 and VG204 sample files.
- File Formats—The Create File Format and Add File Format gateway window now support VG202 and VG204 gateways.
- Generate Gateway Report—The Generate Gateway Report Configuration window now lists all supported gateways, including VG202 and VG204.
- Delete Gateway Support—Delete Gateways Configuration window now lists all BAT-supported gateways, including VG202 and VG204.
- BAT.XLT Support—VG202 and VG204 gateways get supported by BAT.xlt.

Phone Migration in BAT

You can use the Phone Migration feature in Cisco Unified Communications Manager Bulk Administration Tool to migrate phones from one type to another in bulk. You can access the Phone Migration submenu from the Bulk Administration menu of Cisco Unified Communications Manager.

Some limitations that you need to keep in mind when you migrate phones follow:

- Migrating to a phone with fewer speed dials or lines will not remove lines or speed dials; however, some lines/speed dials will no longer display on the phone. You can still find all the original lines/speed dials in the phone configuration window.
- Even migrating to a newer phone can cause loss of features, like in the case of moving from SIP to SCCP or vice versa.
- Only existing phones can get migrated. If you enter a nonexisting device in the CSV file, the system displays an error message.
- If the phone gets migrated successfully, the old phone will get updated with the new phone settings.
- If you select the reset or restart option, the new phone would get reset.

You can create a CSV file for phone migration by using one of the following options:

- Using the BAT Spreadsheet to create CSV Data Files for phone migration
- Using a text editor to create a text-based CSV File for phone migration

Migrating Phones

To migrate phones in bulk with the Phone Migration feature in BAT, use the following procedure:

Before You Begin

- You must have a data file in comma separated value (CSV) format that contains the device name of the phone that you want to migrate, the MAC address for the new phone, and the description for the new phone.
- You must have a phone template of a specific type and the protocol that you want to use for migration configured and ready.
- Upload the data files by choosing the relevant target and function for the transaction by using the procedure that is mentioned in "Uploading a File" section in the *Cisco Unified Communications Manager Bulk Administration Guide*.

Procedure

Step 1 Choose **Bulk Administration > Phone Migration**. The Phone Migration Configuration window displays.

Step 2 You can choose to reset or restart phones by selecting the appropriate radio button from the Reset/Restart Information section. 'Don't Reset/Restart phones' provides the default setting.

Step 3 In the Phone Migration Information section, from the File Name drop-down list box, choose the file that you uploaded.

Step 4 From the Phone Template Name drop-down list box, choose the phone template that you want to use for migration.

Step 5 In the Job Information section, enter a description for the job. The default description specifies Phone Migration.

Step 6 You can choose to run the job immediately or later by selecting the corresponding radio button.

Step 7 To create a job for migrating phones, click **Submit**.

Step 8 A warning message informs you of a possible loss of features/data.

To return to the Phone Migration Configuration window without submitting the job, click **Cancel**;

OR

To continue with submitting the job, click **OK**.

A message in the Status section lets you know that the job was submitted successfully.

Step 9 To schedule and/or activate this job, use the Job Scheduler option in the Bulk Administration main menu.

Support for Geolocations and Logical Partitioning

BAT supports the logical partitioning feature by enabling geolocation configuration in bulk. The following BAT windows include the Geolocation field:

- Bulk Administration > Phones > Phone Template—The GeoLocation drop-down list box displays on the Phone Template Configuration window.
- Bulk Administration > Gateways > Gateway Templates > Select VG224 Gateway, Module: Analog, Subunit0: 24FXS-SCCP, Product Type: Analog—The GeoLocation drop-down list box displays on the Phone Template Configuration window.

New fields That Are Supported for Export by Import/Export

Bulk Administration > Import/Export > Export. The following new fields get supported for export by the Import/Export tool:

System Data

- Geo Location
- Geo Location Filter
- Enterprise Phone Configuration

Call Routing Data

- Logical Partition Policy

Support for Seamless Integration (Apply Config)

BAT supports the seamless integration feature by enabling the Apply Config button in the following windows:

- Bulk Administration > Phones > Update Phones—The **Apply Config** button allows you to reset only the settings that changed since the last reset.
- Bulk Administration > Phones > Reset/Restart Phones—The **Apply Config** button allows you to reset only the settings that changed since the last reset.

Cisco Unified Serviceability

This section provides information on the following topics:

- IPv6 and Serviceability, page 152
- Service Manager Enhancements, page 154
- Audit Logging, page 155
- Alarms, page 156

IPv6 and Serviceability

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, refer to the *Cisco Unified Serviceability Administration Guide*. For information on new and updated alarms, see the "Alarms" section on page 156.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

With Cisco Unified Communications Manager 7.1(2) release, the CTI InetAddress ccmCTIDeviceInetAddressType and ccmCTIDeviceInetAddress fields get deprecated. Two new IPv4/IPv6 fields get added to improve the SNMP query performance when a huge number of entries exist in the table.

The new fields that are added to the ccmCTIDeviceTable in CISCO-CCM-MIB include ccmCTIDeviceInetAddressIPv4 and ccmCTIDeviceInetAddressIPv6. The definitions follow:

```
ccmCTIDeviceInetAddressIPv4 OBJECT-TYPE
SYNTAX          InetAddressIPv4
MAX-ACCESS      read-only
STATUS          current
```

DESCRIPTION—This object identifies the last known primary IPv4 address of the CTI device. This object contains value zero if IPV4 address is not available.

::= { ccmCTIDeviceEntry 14 }

```
ccmCTIDeviceInetAddressIPv6 OBJECT-TYPE
SYNTAX      InetAddressIPv6
MAX-ACCESS     read-only
STATUS      current
```

DESCRIPTION—This object identifies the last known primary IPv6 address of the CTI device. This object contains value zero if IPV6 address is not available.

::= { ccmCTIDeviceEntry 15 }

With these changes, the ccmCTIDeviceEntry looks like the following example:

```
CcmCTIDeviceEntry ::= SEQUENCE {
    ccmCTIDeviceIndex                 CcmIndex,
    ccmCTIDeviceName                  SnmpAdminString,
    ccmCTIDeviceType                  INTEGER ,
    ccmCTIDeviceDescription           SnmpAdminString,
    ccmCTIDeviceStatus                CcmDeviceStatus,
    ccmCTIDevicePoolIndex             CcmIndexOrZero,
    ccmCTIDeviceInetAddressType       InetAddressType,
    ccmCTIDeviceInetAddress           InetAddress,
    ccmCTIDeviceAppInfo               SnmpAdminString,
    ccmCTIDeviceStatusReason          CcmDevFailCauseCode,
    ccmCTIDeviceTimeLastStatusUpdt    DateAndTime,
    ccmCTIDeviceTimeLastRegistered    DateAndTime,
    ccmCTIDeviceProductTypeIndex      CcmIndexOrZero,
    ccmCTIDeviceInetAddressIPv4       InetAddressIPv4,
    ccmCTIDeviceInetAddressIPv6       InetAddressIPv6
}
```

For More Information

- IPv6 and RTMT, page 163
- IPv6 and CDRs, page 169
- IPv6 Support, page 183

Service Manager Enhancements

The following information describes enhancements for Service Manager.

Starting and Stopping Service States

Cisco Unified Communications Manager 7.1(2) includes two new service states: Starting and Stopping.

When the service state is stopping, a service cannot start. When a service state is starting, a service cannot stop. These states display in the Service Activation window in Cisco Unified Serviceabilityand in the command line interface (CLI).

Disaster Recovery System Enhancements for Service Manager

The Disaster Recovery System backs up the services.conf and servM.conf files. The restore process restores all services to their original forms.

Single Tomcat Session

Instead of creating a new session on the Tomcat manager webapp for every Tomcat request, service manager now creates a single session on the Tomcat manager webapp.

Security Enhancements

Service Manager listens to port 8889 at the local host.

Service Manager Return Codes

Table 27 describes the Service Manager return codes that Release 7.1(2) implements.

Table 27 New Service Manager Return Codes

Code	Meaning
1078	Service start pending
1079	Service stop pending
1080	HTTP timed out
1081	Tomcat webapp deploy failed
1082	Invalid Tomcat application URL
1083	No such Tomcat command specified
1084	Tomcat webapp undeploy failed
1085	No such Tomcat manager user failed
1086	Tomcat manager failed to reload
1087	Tomcat manager failed
1088	Webapp start failed

Table 27 New Service Manager Return Codes (continued)

Code	Meaning
1089	Unknown Tomcat command
1090	Connection refused

Audit Logging

Centralized audit logging ensures that configuration changes to the Cisco Unified Communications Manager system get logged in separate log files for auditing. The following four types of logs get saved to three folders in RTMT:

- Application—Reports application configuration changes for RTMT, Cisco Unified Serviceability, CAR, the CLI, and Cisco Unified Communications Manager Administration. Although it stays enabled by default, you can configure it in Cisco Unified Serviceability by choosing **Tools > Audit Log Configuration**.
- Database—Reports database changes. This log does not get enabled by default. Configure this log in Cisco Unified Serviceability by choosing **Tools > Audit Log Configuration**. In this window, scroll to Database Audit Log Filter Settings to enable the audit logging and specify the debug audit level as Schema Only, Administrative Tasks, Database Updates, or Database Reads. This audit differs from the Application audit because it logs database changes, and the Application audit logs application configuration changes.
- Operating System—Reports events that are triggered by the operating system. It does not get enabled by default. The **utils auditd** CLI command enables, disables, or gives status about the events. See the "New Commands and Parameters" section on page 26 for information about using the command.
- Remote Support Acct Enabled—Reports CLI commands that get issued by technical support teams. You cannot configure it, and the log gets created only if the Remote Support Acct gets enabled by the technical support team.

Access the audit logs in RTMT in Trace and Log Central. Go to **System > Real-Time Trace > Audit Logs > Nodes**. After you select the node, another window displays System > Cisco Audit Logs. The logs get stored in one of the following folders:

- AuditApp (application)—Created by default. Audit logs get enabled by default in Cisco Unified Serviceability. If the audit logs get disabled in Cisco Unified Serviceability, no new audit log files get created.

  AuditApp creates one log file until the configured maximum file size is reached; then, it closes and creates a new log file. If the system specifies rotating the log files, AuditApp saves the configured number of files. You can view some of the logging events by using RTMT SyslogViewer.
- informix (database)—Enabled in Cisco Unified Serviceability under Tools > Audit Log Configuration. The folder does not display unless the audit is enabled.
- vos (operating system and remote support)—Enabled with the **utils auditd** CLI command. The folder does not display unless the audit is enabled.

For events that get logged, see the "Audit Logs in RTMT" section on page 166.

Audit logging contains the following parts:

- Audit logging framework—The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different Cisco Unified Communications Manager components provide their own logging.

The following example displays an API that a Cisco Unified Communications Manager component can use to send an alarm:

```
User ID: CCMAdministrator
Client IP Address: 172.19.240.207
Severity: 3
EventType: ServiceStatusUpdated
ResourceAccessed: CCMService
EventStatus: Successful
Description: CallManager Service status is stopped
```

- Audit event logging—An audit event represents any event that is required to be logged. The following Cisco Unified Communications Manager components generate audit events:
  - Cisco Unified Communications Manager Administration
  - Cisco Unified Serviceability Administration
  - Cisco Unified Real-Time Monitoring Tool (RTMT)
  - Cisco Unified CDR Analysis and Reporting (CAR)

  The following example displays a sample audit event:

  ```
  CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
  UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
  EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
  Successful Description: Call Manager Service status is stopped App ID:Cisco Tomcat
  Cluster ID:StandAloneCluster Node ID:sa-cm1-3
  ```

The Cisco Audit Event Service displays in Control Center—Network Services in Cisco Unified Serviceability, so you can start or stop the Audit Log service. To access this service, choose **Tools** > **Control Center—Network Services**.

To configure audit logging in Cisco Unified Serviceability, choose **Tools > Audit Log Configuration**. Use the Audit Log Configuration window to configure the settings for the Cisco Unified Communications Manager application audit logs. For a description of the settings that you can configure for audit log configuration, refer to the *Cisco Unified Serviceability Administration Guide*.

Tip Only a user with an audit role has permission to change the Audit Log settings. By default, the CCMAdministrator has the audit role after fresh installs and upgrades. The CCMAdministrator can assign the “standard audit users” group to a new user that the CCMAdministrator specifically creates for audit purposes. The CCMAdministrator can then be removed from the audit user group. The “standard audit log configuration” role provides the ability to delete audit logs, read/update access to Cisco Unified Real-Time Monitoring Tool, Trace Collection Tool, RTMT Alert Configuration, the Control Center - Network Services window, RTMT Profile Saving, the Audit Configuration window, and a new resource called Audit Traces.

For More Information

- Alarms, page 156
- Audit Logs in RTMT, page 166
- Audit Events Get Logged for CAR, page 168

Alarms

Cisco Unified Serviceability contains the following new alarm catalogs:

- System Alarm Catalog—CDPAlarmCatalog

- CallManager Alarm Catalog—Phone

The following section contains information on updated and new alarms:

Refer to the *Cisco Unified Serviceability Administration Guide* for information on alarm definitions and for information on how to configure alarms.

kCtiProviderOpenFailure (Updated)

This alarm indicates that the CTI application failed to open provider. If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
- Severity—Error (3)
- New Parameter—IPV6Address(String)

kCtiProviderClosed (Updated)

This alarm indicates that CTI application connection is closed. If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
- Severity—Informational (6)
- New Parameter—IPV6Address(String)

kCtiProviderOpened (Updated)

This alarm indicates that the CTI application connection opened. If your network supports, IPv6, this alarm may contain an IPv6 address.

- Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
- Severity—Informational (6)
- New Parameter—IPV6Address(String)

kCtiIncompatibleProtocolVersion (Updated)

This alarm indicates that the The JTAPI/TAPI application version is not compatible with this version of CTIManager. If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Catalog—Choose CallManager > CtiManagerAlarmCatalog.
- Severity—Error (3)
- New Parameter—IPV6Address(String)

DeviceRegistered (Updated)

This alarm indicates that a device successfully registered with Cisco Unified Communications Manager. If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Definition Catalog—Choose CallManager Alarm Catalog > CallManager.
- Severity—Informational (6)
- New Parameters
  - IPV6Address[Optional].[String]
  - IPAddressAttributes[Optional].[Enum]
  - IPV6AddressAttributes [Optional].[Enum]
  - ActiveLoadId [Optional].[String]
- New Enum Definitions for IPAddrAttributes
  - 0—Unknown
  - 1—Administrative only
  - 2—Signal only
  - 3—Administrative and signal
- New Enum Definitions for IPV6AddrAttributes
  - 0—Unknown
  - 1—Administrative only
  - 2—Signal only
  - 3—Administrative and signal

DeviceUnregistered (Updated)

This alarm indicates that a device that was previously registered with Cisco Unified Communications Manager unregistered. This event may get issued as part of normal unregistration event or due to some other reason such as loss of keepalives. In cases of normal unregistration, if the Reason Code is CallManagerReset, CallManagerRestart, or DeviceInitiatedReset, the alarm severity gets lowered to Informational (6).

If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Definition Catalog—Choose CallManager Alarm Catalog > CallManager.
- Severity—Error (3)
- New Parameters
  - IPV6Address [Optional].[String]

    - IPAddressAttributes [Optional].[Enum]
    - IPV6AddressAttributes [Optional].[Enum]
- New Enum Definitions for IPAddrAttributes
    - 0—Unknown
    - 1—AdministrativeOnly
    - 2—SignalOnly
    - 3—AdministrativeAndSignal
- New Enum Definitions for IPV6AddrAttributes
    - 0—Unknown
    - 1—Administrative only
    - 2—Signal only
    - 3—Administrative and signal

DeviceTransientConnection (Updated)

This alarm indicates that a transient connection attempt occurred. A connection got established and immediately dropped before completing registration. Incomplete registration may indicate that a device is rehoming in the middle of registration. The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.

If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Definition Catalog—CallManager Alarm Catalog > CallManager
- Severity—Error (3)
- New Parameters
    - IPV6Address [Optional].[String]
    - IPAddressAttributes [Optional].[Enum]
    - IPV6AddressAttributes [Optional].[Enum]
- Enum Definitions for IPAddrAttributes
    - 0—Unknown
    - 1—AdministrativeOnly
    - 2—SignalOnly
    - 3—AdministrativeAndSignal
- Enum Definitions for IPV6AddrAttributes
    - 0—Unknown
    - 1—AdministrativeOnly
    - 2—SignalOnly
    - 3—AdministrativeAndSignal

SIPStarted (Updated)

This alarm indicates that Cisco Unified Communications Manager is ready to handle calls for the indicated SIP device. This alarm does not indicate the current state of the SIP device, only that Cisco Unified Communications Manager is prepared to handle calls to/from the SIP device.

If your network supports IPv6, this alarm may contain an IPv6 address.

- Alarm Definition Catalog—Choose CallManager Alarm Catalog > CallManager.
- Severity—Informational (6)
- New Parameter—IPV6Address[Optional].[String]

ServiceStarted (Updated)

If your network supports IPv6, this alarm may contain an IPv6 address.

This alarm indicates that the service started.

- Alarm Definition Catalog—Choose System Alarm Catalog > GenericAlarmCatalog.
- Severity—Informational (6)
- New Parameter—IPV6Address[Optional](String)

AuditEventGenerated (New)

This alarm indicates that the application generated an audit event to the audit log.

- Alarm Definition Catalog—Choose System Alarm Catalog > GenericAlarmCatalog.
- Severity—Informational (6)
- Parameters
  - UserID (String)
  - ClientAddress (String)
  - Severity (String)
  - EventType (String)
  - ResourceAccessed(String)
  - EventStatus (String)
  - AuditDetails (String)
  - ComponentID (String)

DUPLEX_MISMATCH (New)

This alarm gets generated by Cisco CDP whenever a duplex mismatch occurs between the local interface and switch interface.

- Alarm Definition Catalog—Choose System Alarm Catalog > CDPAlarmCatalog.
- Severity—Critical (2)
- Parameters
  - Switch Duplex Settings(String)
  - Local Interface Duplex Settings(String)

- Recommended Action—Ensure that duplex settings are set to auto or full on local interface as well as switch interface.

DeviceImageDownloadFailure (New)

This alarm gets generated when a Cisco Unified IP Phone failed to download its image.

- Alarm Definition Catalog—CallManager Alarm Catalog > Phone
- Severity—Warning (4)
- Parameters
  - DeviceName(String)
  - IPAddress(String)
  - Active(String)
  - Inactive(String)
  - FailedLoadId(String)
  - Method(Enum)
  - FailureReason(Enum)
  - Server(String)
- Enum Definitions for Method
  - 1—TFTP
  - 2—HTTP
  - 3—PPID
- Enum Definitions for FailureReason
  - 1—TFTP server returned specific error text
  - 2—File Not Found
  - 3—Internal Phone Error
  - 4—TftpClient could not write out the results
  - 5—Encryption error
  - 6—File not encrypted
  - 7—Encryption key mismatch
  - 8—Decryption failed
  - 9—No Tftp server set
  - 10—Illegal tftp operation
  - 11—File already exists
  - 12—No such user
  - 13—Exceeded max waiting time for status
  - 14—Data block received from Tftp was too short
  - 15—Data block received from Tftp was too long
  - 16—Network is down
  - 17—DNS Name for this server could not be resolved

  - 18—No DNS Server
  - 19—TFTP Timeout
- Recommended Action—Verify the following information:
  - Image Download Server IP address or hostname is correct. If you are using a hostname, verify the Domain Name Server (DNS) is accessible from the phone and can resolve the hostname.
  - TFTP service is activated and running on the Image Download Server. Verify the Image Download Server is accessible from the phone.
  - Device configured.

DeviceImageDownloadStart (New)

Cisco Unified IP Phone has started downloading its image.

- Alarm Definition Catalog—Choose CallManager Alarm Catalog > Phone.
- Severity—Informational (6)
- Parameters
  - DeviceName(String)
  - IPAddress(String)
  - Active(String)
  - RequestedLoadId(String
- Recommended Action—No action is required.

DeviceImageDownloadSuccess (New)

Cisco Unified IP Phone has successfully downloaded its image.

- Alarm Definition Catalog—CallManager Alarm Catalog > Phone
- Severity—Informational (6)
- Parameters
  - DeviceName(String)
  - IPAddress(String)
  - Method(Enum)
  - Active(String)
  - Inactive(String)
  - Server(String)
- Recommended Action—No action is required.

DeviceApplyConfigResult (New)

Cisco Unified IP Phone has applied its configuration.

- Alarm Definition Catalog—Choose CallManager Alarm Catalog > Phone.
- Severity—Informational (6)
- Parameters
  - DeviceName(String)

  - IPAddress(String)
  - CUCM_Result(String)
  - Phone_Result(String)
  - Reason(String)
- Recommended Action—No action is required.

Cisco Unified Cisco Unified Real-Time Monitoring Tool

This section contains these subsections:

- IPv6 and RTMT, page 163
- Alerts, page 163
- Performance Monitoring Counters, page 164
- Trace and Log Central, page 165
- Quality Report Tool Reports, page 167

IPv6 and RTMT

In RTMT, you can search for and monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the application, device, or line, enter the IPv6 address and check the AppIpv6Addr check box in the attribute window.

In addition, you can perform a device search on phones or SIP trunks that use IPv6 addresses. When you choose CallManager > Device Search > Open Device Search > Phones (or SIP Trunks), make sure that you specify an IPv6 address and check the IPv6Address check box in the attributes window.

Tip IP Subnet does not apply for IPv6 search criteria.

For More Information

- IPv6 and Serviceability, page 152
- Alarms, page 156
- Performance Monitoring Counters, page 164
- Log Files and IPv6, page 167
- IPv6 and CDRs, page 169

Alerts

Cisco Unified Communications Manager Release 7.1(2) provides the following new or updated alerts:

- DBReplicationTableOutOfSync— Cisco Unified Communications Manager Releases 6.1(3) and 7.1(2) introduce this alert. For information on the DBReplicationTableOutofSync alert, see the "Table Out of Sync Detection" section on page 136.

Performance Monitoring Counters

The following performance monitoring counter updates exist in Cisco Unified Real-Time Monitoring Tool for Cisco Unified Communications Manager 7.1(2):

- Logical Partitioning, page 164
- IPv6, page 164

Logical Partitioning

The Cisco Call Restriction counters specify a new group of performance monitoring counters that log the number of failures that result because of logical partitioning policy restrictions. The Cisco Call Restriction counters include the following performance monitoring counters:

- AdHocConferenceFailures
- BasicCallFailuresNoForwardingFailures
- LogicalPartitionFailuresTotal
- MeetMeConferenceFailures
- MidCallFailures
- ParkRetrievalFailures
- PickUpFailures
- SharedLineFailures
- TransferFailures

IPv6

In RTMT, the performance monitoring counters in Table 28 display for the IP6 object, which provides information on the IPv6-related statistics for your system.

Table 28 IP6

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated as a result of fragmentation at this entity.
Frag Fails	This counter represents the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not, for example, because their Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that have been successfully fragmented at this entity.
In Delivers	This counter represents the total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol [ICMP]).
In Discards	This counter represents the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams that were discarded while awaiting reassembly.

Table 28 IP6 (continued)

Counters	Counter Descriptions
In HdrErrors	This counter represents the number of input datagrams that were discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
In Receives	This counter represents the number of input datagrams that were received from all network interfaces, including those received with errors.
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the total number of IP datagrams that were received and the number of IP datagrams sent.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. One reason may represent a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams that local IP user-protocols (including Internet Control Message Protocol [ICMP]) supply to IP in requests transmission. This counter does not include any datagrams that are counted in ForwDatagrams.
Reasm Fails	This counter represents the number of failures that are detected by the IP reassembly algorithm (for various reasons, for example, timed out, errors, and so on). This does not necessarily represent a count of discarded IP fragments because some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that needed to be reassembled at this entity.

Trace and Log Central

This section contains information on the following topics:

- System History Log Displays in RTMT, page 165
- Audit Logs in RTMT, page 166
- Log Files and IPv6, page 167

System History Log Displays in RTMT

Cisco Unified Communications Manager Releases 6.1(3) and 7.1(2) introduce the system history log.

To access the system history log in RTMT, navigate to RTMT Trace Collection:

RTMT > Trace Log Collection

For more information on the system history log, see the "System History Log for Cisco Unified Communications Manager" section on page 19.

Audit Logs in RTMT

Tip See "Audit Logging" section on page 155 for information about the location of the log files, how to access the files, and how to configure the logging.

With audit logging, any configuration change to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged.

The following events get logged for various components of Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts).
- User role membership updates (user added, user deleted, user role updated).
- Role updates (new roles added, deleted, or updated).
- Device updates (phones and gateways).
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and Cisco Unified Communications Manager server additions or deletions).

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR Management.
- Review of any report in the Serviceability Reports Archive. View this log on the reporter node.

Cisco Unified Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Cisco Unified Communications Manager CDR Analysis and Reporting creates audit logs for the following events:

- Scheduling the CDR Loader.

- Scheduling the daily, weekly, and monthly user reports, system reports, and device reports.
- Mail parameters configurations.
- Dial plan configurations.
- Gateway configurations.
- System preferences configurations.
- Autopurge configurations.
- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configurations.

All audit logs get collected, viewed and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.

Audit logs get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Audit User Configuration window in Cisco Unified Serviceability. In RTMT, choose **Trace and Log Central > Audit Logs**.The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Log Files and IPv6

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

Quality Report Tool Reports

A change occurred in the Call State information that is collected from Cisco Unified Communications Manager/CTIManager and displayed in the Quality Report Tool (QRT) reports. Prior to Release 7.1(2), the information included Connected, Connected Conference, Connected Transfer, and On Hook call state information. Now, the report only includes Connected and On Hook call state information.

Cisco Unified Communications Manager CDR Analysis and Reporting

This section contains these subsections:

Audit Events Get Logged for CAR

Centralized audit logging ensures that a configuration change to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged. For information on the events that get logged for CAR, see the "Audit Logs in RTMT" section on page 166.For information about event logging, see the "Audit Logging" section on page 155.

Customized Log-on Message

You can upload a text file that contains a customized log-on message that displays in the initial Cisco Unified Communications Manager CDR Analysis and Reporting window.

Upgrade of CAR Data

Be aware that when you upgrade from an earlier version of Cisco Unified Communications Manager to a later version of Cisco Unified Communications Manager, you may not be able to upgrade all your CDR data.

The Cisco Unified Communications Manager installation program limits the time for the migration of the CAR records from the CSV files in the Data Migration Assistant (DMA) TAR file to the CAR database on the upgraded system. The migration time equals 60 minutes. To allow the migration of the highest number of CSV files in the allotted time, CAR record migration uses the following steps:

- Data migration begins with the migration of the billing records from the tbl_billing_data CSV file to the tbl_billing_data table of the CAR database. Data migration begins with the newest record and proceeds toward the oldest record in the CSV file. The billing data migration stops when no more billing records exist to migrate or when the migration time reaches 60 minutes.
- If time remains after the billing data gets migrated, data migration proceeds with the migration of error records from the tbl_billing_error CSV file to the tbl_billing_error table of the CAR database. Data migration begins with the newest record and proceeds toward the oldest record in the CSV file. For each error record that gets migrated, CAR migrates the data that corresponds to the error_record_id that is present in the tbl_error_id_map CSV file into the tbl_error_id_map table of the CAR database. This action ensures that error record data migration stays consistent with data in the tbl_error_id_map. The error record data migration stops when no more error records to migrate exist or when the migration reaches 60 minutes.

If the 60-minute migration time limit occurs at any point in the migration process, CAR data migration ceases, and the tbl_system_preferences of the CAR database gets updated to reflect the data that are present in the upgraded system database.

Backup of CAR Data

The CAR and CDR Disaster Recovery Service (DRS) now integrates into the Cisco Unified Communications Manager DRS. The DRS includes the backup of the CAR database, pregenerated reports, and the CDR preserved flat files.

The CAR Web Service and CAR Scheduler automatically stop before the backup and restore process begins and automatically restart after the backup and restore process completes.

Table 1-29 displays the features and components that the Disaster Recovery System can back up and restore. For each feature that you choose, the system backs up all its components automatically.

Table 1-29 Cisco Unified CM Features and Components

Feature	Components
CCM—Cisco Unified Communications Manager	Cisco Unified Communications Manager database
	Platform
	Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDRs)
	CDR Reporting and Analysis (CAR)

Ensure CAR Administrator Privileges Are Restored After Upgrade

When you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. You must reset the CAR administrator privileges after the upgrade. Refer to the “Configuring CAR Administrators, Managers, and Users” section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.

Cisco Unified Communications Manager Call Detail Records

This section contains these subsections:

- IPv6 and CDRs, page 169
- H.239 and CDRs, page 171
- Logical Partitioning, page 173
- New Call Termination Cause Codes, page 173
- SIP Calls with URL in callingPartyNumber Field, page 173
- GlobalCallId Survives Over Cisco Unified Communications Manager Restarts, page 173

IPv6 and CDRs

Cisco Unified Communications Manager Release 7.1(2) supports IPv6. Table 30 describes the CDRs that are related to IPv6.

Table 30 IPv6 CDR Field Descriptions

Field Name	Range of Values	Description
origIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that originates the call signalling. The field can represent either IPv4 or IPv6 format, depending on the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field specifies the address of the Cisco Unified IP Phone. For PSTN calls, this field specifies the address of the gateway. For intercluster calls, this field specifies the address of the remote Cisco Unified Communications Manager. The IP address comprises either dotted decimal format or colon-separated hexadecimal format. Default - The IP address of the originating device gets reported by the device or used for the call after media negotiation.
destIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that terminates the call signalling. The field can comprise either IPv4 or IPv6 format, depending upon the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field specifies the address of the Cisco Unified IP Phone. For PSTN calls, this field specifies the address of the gateway. For intercluster calls, this field specifies the address of the remote Cisco Unified Communications Manager. The IP address comprises either dotted decimal format or colon-separated hexadecimal format. Default - Empty String "" or null. If the destination does not get reached, this field stays empty.

H.239 and CDRs

Cisco Unified Communications Manager Release 7.1(2) supports H.239. This feature defines the procedures for the use of up to two video channels in H.320-based systems and for labeling individual channels with a “role” (presentation or live). Requirements exist for processing both the channel and the role of the channel content in the call. Role labels apply to both H.320 and H.245 signaling-based systems.

Table 31 describes the CDR fields that support a second video channel for both the origination and destination devices.

Table 31 H.239 CDR Field Descriptions

Field Name	Range of Values	Description
origVideoCap_Codec_Channel2	0, 100 = H.261, 101 = H.263, 102 = Vieo, 103 = H.264,	This field identifies the codec type that the originator uses to transmit video (H.261, H.263, Vieo, H.264) for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
origVideoCap_Bandwidth_Channel2	0, Positive integer	This field identifies the bandwidth, measured in units of kbps, for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
origVideoCap_Resolution_Channel2	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16	This field identifies the video resolution for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
origVideoTransportAddress_IP_Channel2	0, Integer	This field identifies the v4 IP address of the device that originates the call for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.

Table 31 H.239 CDR Field Descriptions (continued)

Field Name	Range of Values	Description
origVideoTransportAddress_Port_Channel2	0, Positive integer	This field identifies the video RTP port that is associated with the origH239VideoTransportAddress_IP field for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
origVideoChannel_Role_Channel2	0 = Presentation role, 1 = Live role, Positive integer	This field identifies the H.239 video channel role of the device that originates the video. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
destVideoCap_Codec_Channel2	0, 100 = H.261 101 = H.263 102 = Vieo 103 = H.265	This field identifies the codec type that the terminating party uses to transmit video for the second video channel (H.261, H.263, Vieo, H.264). Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
destVideoCap_Bandwidth_Channel2	0, Positive integer	This field identifies the bandwidth, measured in units of kbps, for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
destVideoCap_Resolution_Channel2	0, 1 = SQCIF, 2 = QCIF, 3 = CIF, 4 = CIF4, 5 = CIF16	This field identifies the video resolution for the second video channel. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
destVideoTransportAddress_IP_Channel2	0, Integer	This field identifies the v4 IP address of the device that receives the call. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.

Table 31 H.239 CDR Field Descriptions (continued)

Field Name	Range of Values	Description
destVideoTransportAddress_Port_Channel2	0, Positive integer	This field identifies the video RTP port that is associated with the destH239VideoTransportAddress_IP field. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.
destVideoChannel_Role_Channel2	0 = Presentation role, 1 = Live role, Positive integer	This field identifies the H.239 video channel role of the device that receives the call. Default - 0. If media does not get established, this field displays 0. Also, if H.239 is not supported, this field displays 0.

Logical Partitioning

Cisco Unified Communications Manager Release 7.1(2) supports logical partitioning. CDR examples that use logical partitioning get provided for call termination cause code 424 and cause code 503.

New Call Termination Cause Codes

Table 32 describes new Cisco-specific call termination cause codes for logical partitioning.

Table 32 Cisco-Specific Call Termination Cause Codes

Decimal Value Code	Hex Value Code	Description
419430421	0x19000015	CCM_SIP_424_BAD_LOCATION_INFO
-1493172161	0xA700003F	CCM_SIP_503_SERVICE_UNAVAILABLE_SER_OPTION_NOAVAIL

SIP Calls with URL in callingPartyNumber Field

A new CDR example applies for this situation: an incoming call is received through a SIP trunk by the Cisco Unified Communications Manager. The call contains a SIP URL for the callingPartyNumber CDR field.

GlobalCallId Survives Over Cisco Unified Communications Manager Restarts

For Cisco Unified Communications Manager Release 5.x and later releases, the value in the GlobalCallId CDR field survives over Cisco Unified Communications Manager restarts. In Release 4.x and earlier releases, even though the GlobalCallId field is time-based, the field gets reused under conditions of heavy traffic. Because of this behavior, problems can occur with customer billing applications and the ability of CAR to correlate CMRs with CDRs and to correlate conference call

CDRs. For Release 5.x and later releases, GlobalCallId redesign ensures the field retains a unique value, at least for a certain number of days. Now, the last used globalCallId_callId value gets written to disk periodically (for every x number of calls). The value gets retrieved after a Cisco Unified Communications Manager restart, and the new globalCallId_callId value begins with this number plus x.

Cisco Unified Reporting

For a complete description of reports that are available on your system and the data that gets captured in a report, access the **Report Descriptions** report, as described in the *Cisco Unified Reporting Administration Guide*.

Table 33 describes the standard reports that display in Cisco Unified Reporting after a Cisco Unified Communications Manager upgrade/installation.

Table 33 Standard Reports That Display in Cisco Unified Reporting

Report	Description
Unified CM Cluster Overview	Provides an overview of the Cisco Unified Communications Manager cluster; for example, this report provides the Cisco Unified Communications Manager version that is installed in the cluster, the host name or IP address of all servers in the cluster, a summary of hardware details, and so on.
Unified CM Data Summary	Provides a summary of data that exists in the Cisco Unified Communications Manager database, according to the structure of the menus in Cisco Unified Communications Manager Administration. For example, if you configure 3 credential policies, 5 conference bridges, and 10 shared line appearances, you can see that type of information in this report.
Unified CM Database Replication Debug	Provides debugging information for database replication. **Tip** For this report, generation takes up to 10 seconds per server in the cluster and may spike CPU.
Unified CM Database Status	Provides a snapshot of the health of the Cisco Unified Communications Manager database. Generate this report before an upgrade to ensure that the database is healthy.
Unified CM Device Counts Summary	Provides the number of devices by model and protocol that exist in the Cisco Unified Communications Manager database.
Unified CM Extension Mobility	Provides a summary of Cisco Extension Mobility usage; for example, the number of phones that have a Cisco Extension Mobility user logged in to them, the users that are associated with Cisco Extension Mobility, and so on.
Unified CM GeoLocation Policy [new for Release 7.1(2)]	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix.
Unified CM GeoLocation Policy with Filter [new for Release 7.1(2)]	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix for the selected GeoLocation policy.
Unified CM Lines Without Phones	Provides a list of lines that are not associated with a phone.
Unified CM Multi-Line Devices	Provides a list of phones with multiple line appearances.

Table 33 Standard Reports That Display in Cisco Unified Reporting (continued)

Report	Description
Unified CM Phone Feature List [new for Release 7.1(2)]	Provides a list of supported features for each device type in Cisco Unified Communications Manager Administration.
Unified CM Phones With Mismatched Load [new for Release 7.1(2)]	Provides a list of all phones that have mismatched firmware load.
Unified CM Phones Without Lines	Provides a list of all phones in the Cisco Unified Communications Manager database that do not have lines associated with them.
Unified CM Shared Lines	Provides a list of all phones in the Cisco Unified Communications Manager with at least one shared line appearance.
Unified CM Table Count Summary	Provides a database centric view of data. This report proves useful for administrators or AXL API developers that understand database schema.
Unified CM User Device Count	Provides information about associated devices; for example, this report lists the number of phones with no users, the number of users with 1 phone, and the number of users with more than 1 phone.
Unified CM Voice Mail	Provides a summary of voice-messaging related configuration in the Cisco Unified Communications Manager Administration; for example, this report lists the number of configured voice mail ports, the number of message waiting indicators, the number of configured voice messaging profiles, the number of directory numbers that are associated with voice message profiles, and so on.
Unified CM Device Distribution Summary	Provides a summary of how devices are distributed throughout the cluster; for example, this report shows which devices are associated with the primary, secondary, tertiary servers and so on.

APIs

This section describes the new and changed API features in Cisco Unified Communications Manager Release 7.1(2). It contains the following sections:

- Cisco Unified TAPI Service Provider (TSP), page 175
- Cisco Unified JTAPI, page 177
- Skinny Client Control Protocol (SCCP), page 179
- Administrative XML (AXL) Programming, page 180
- Serviceability XML Programming, page 183

Cisco Unified TAPI Service Provider (TSP)

This section describes the new and changed features that are supported in TAPI for Cisco Unified Communications Manager Release 7.1(2).

IPv6 Support

Cisco Unified Communications Manager supports IPv6 addresses in its network. Use of IPv6 increases the number of addresses that are available for devices in the network. TAPI can connect to Unified CM with IPv6 support if the IPv6 Support feature is enabled on Unified CM. The following enhancements that have been made to Cisco Unified Communications Manager support IPv6:

- Provides the IPv6 address of the calling party to the called party in the Devspecific part of LINECALLINFO.
- Provides support to register a CTI port or a route point that has an IPv6 address.
- Ensures the RTP destination address also contains IPv6 addresses if the same is involved in media establishment.

The TSP user interface includes the primary and backup CTI Manager address and a flag that indicates the preference of user while user is connecting to the CTI Manager. You can register CTI ports and route points can be registered with IPv4, IPv6, or both.

The following new CiscoLineDevSpecific functions allow the application to terminate media by using IPv6 address:

- CciscoLineDevSpecificSetIPv6AddressAndMode – Allows the application to specify IP address mode and IPv6 address before CTI port and route point are opened.
- CciscoLineDevSpecificSetRTPParamsForCallIPv6 – Allows application to set receiving IPv6 address/port in responding to SLDSMT_OPEN_LOGICAL_CHANNEL event in the case of dynamic port registration.

Be aware that Extension 0x00090000 must be negotiated to support the feature.

Direct Transfer Across Lines Support

The Direct Transfer Across Lines feature allows the application to directly transfer calls across the lines that are configured on the device. The application must monitor both lines when the calls are directly transferred across lines.

A new LineDevSpecific extension, CciscoLineDevSpecificDirectTransfer, can direct transfer calls across the lines or on the same line. Be aware that Extension 0x00090000 must be negotiated to use CciscoLineDevSpecificDirectTransfer.

Device State Server Support

Device State Server feature provides accumulative State of all the lines on the device. Applications get notified about the device status through PHONE_DEVSPECIFIC and LINE_DEVSPECIFIC Events.

For an application to enable the Device State Server Support, it needs to set the DEVSPECIFIC_DEVICE_STATE and DEVSPECIFIC_DEVICE_STATE_STATUS_ message flag by means of the lineDevSpecific SLDST_SET_STATUS_MESSAGES request and PhoneDevSpecific CPDST_SET_DEVICE_STATUS_MESSAGES request, respectively.

TAPI will provide notification of the device state of the device to its applications through PHONE_DEVSPECIFIC and LINE_DEVSPECIFIC events.

The possible device states that are delivered to an application from TSP include ACTIVE, ALERTING, HELP, WHISPER, and IDLE.

Drop-Any-Party Support

The Drop-Any-Party feature enables the application to drop any call from the ad hoc conference. This feature currently gets supported from the phone interface. The application uses the LineRemoveFromConference function to drop the call from a conference. When the call is dropped from a conference, the TSP receives CtiDropConferee as the call state change cause, and this gets sent to TAPI as the default cause.

Logical Partitioning Support

The Logical Partitioning feature restricts VoIP to PSTN calls, and vice versa, based on the logical partitioning policy. Any request that interconnects a VOIP call to a PSTN call, or vice versa, in two different geographical locations fails, and the error code gets sent back to the applications.

The device, device pool, trunk, and gateway windows now provide configuration to select geolocation values and construction rules for geolocation strings.

A new enterprise parameter for this feature includes the following values:

- Name: Logical partitioning enabled
- Values: True or False
- Default: False

This release adds the following error code for this feature:
LINEERR_INVALID_CALL_PARTITIONING_POLICY 0xC000000C

Cisco Unified JTAPI

This section describes the new and changed features that are supported in JTAPI for Cisco Unified Communications Manager Release 7.1(2).

Drop Any Party

This feature provides the capability to drop any participants from a conference call. JTAPI allows applications to drop participants from conference by using the existing interface Connection.disconnect() even if the application is not observing the address for the connection. Previously, applications could only disconnect connections for which Address is an observed Address.

Feature behavior varies based on the settings for the Unified CM service parameter Advanced Ad Hoc Conference Enabled. If this service parameter is set to False, applications can drop connections for an unobserved address in a conference call only if the application observes the conference controller address. If this parameter is set to True, applications can drop connections without any restriction.

JTAPI provides an interface on CiscoConnection to get an array of CiscoPartyInfo objects for the connection. CiscoPartyInfo gets used to disconnect participants from a conference by using a new interface, disconnect(), that is provided on CiscoConnection. A normal line includes only one CiscoPartyInfo on its connection, but a shared-line has one CiscoPartyInfo for each line in the shared-line. This enables applications to selectively disconnect a shared line participant if more than one shared line participants is in the conference call. Because shared line participants have only one connection, if the application uses the existing Connection.disconnect() API, it drops all the shared line participants.

JTAPI provides an interface setDropAnyPartyEnabled() on CiscoJtapiProperties to enable or disable this feature and by default, it stays enabled. Alternatively, applications can have the JTAPI ini parameter dropAnyPartyEnabled=0 in jtapi.ini file to disable Drop Any Party feature and dropAnyPartyEnable=1 to enable this feature. If dropAnyPartyEnable parameter is not present in jtapi.ini file, the feature stays enabled by default.

JTAPI also provides an interface, isConferenceCall(), on CiscoCall to determine whether a call is a conference call. This simple method returns a Boolean result.

IPv6 Support

This feature provides support for IPv6 addresses, and Cisco JTAPI gets enhanced to support IPv6 connectivity to CTIManager. It allows JTAPI applications to see IPv6 Address as the calling party address if the feature is enabled and if the Calling Party is an IPv6-enabled phone. With this feature, the following functions get supported:

- Cisco JTAPI exposes new API canSupportIPv6() on CiscoProviderCapabilities Interface to indicate whether Unified CM configuration supports IPv6
- Cisco JTAPI closes media or route terminal if a mismatch exists between what is registered before and what is configured now. CiscoTermRegistrationFailedEv with a new reason code IP_ADDRESSING_MODE_ MISMATCH will get sent under the scenario
- API getIPAddressingMode() on CiscoTerminal Interface exposes the IP Address capability of the terminal. All CiscoTerminal/CiscoMediaTerminal and CiscoRouteTerminal make this capability available.
- IPv6 calling party IP address gets provided through Cisco extensions of CallCtlConnOfferedEv and RouteEvent in an InetAddress object along with the IPv4 address for IPv4 enabled devices.

RTP Address in CiscoRTPOutputStartedEv and CiscoRTPInputStartedEv will also include an IPv6 address in case the observed device is an IPv6 device. That is, API getLocalAddress() on CiscoRTPInputProperties and API getRemoteAddress() on CiscoRTPOutputProperties can now return an IPv6 format IP Address. The API will return an InetAddress object; applications can check whether it is an instance of Inet4Address or Inet6Address to see whether it is an IPv4 or IPv6 format IP address.

Direct Transfer Across Lines

The Direct Transfer Across Lines feature allows support for transfer across lines. It allows two calls on different addresses of the same terminal to be transferred though the Transfer softkey on the phone or transfer() API that is provided by JTAPI and Transfer softkey on certain newer phones. When a transfer is done across lines, the behavior to JTAPI applications changes, as applications do not see a common controller address in final and consult calls. No change occurs in the API, and the same events get delivered whether calls are transferred on the same address (regular transfer) or across addresses (Direct Tx across lines). This feature gets supported on all supported phones – including CTI port, SCCP devices, and SIP devices.

If observer is not added on either of the two addresses across which Transfer is being attempted from JTAPI API, JTAPI throws PlatformException with error: Transfer controller does not get set and could not find a suitable TerminalConnection.

Join Across Lines or Connected Conference Across Lines

User experience gets enhanced in Cisco Unified Communications Manager Release 7.1(2) by introducing new phones that fall outside the purview of existing Join Across Lines feature always Enabled without any service parameter. For these devices, the features remains Enabled to turn it off.

Enhanced MWI

The Enhanced MWI feature allows applications to provide the following message counts to be displayed on phones that support the enhanced message waiting counts:

- Total number of new voice messages (includes normal and high priority messages)
- Total number of old voice messages (includes normal and high priority messages)
- Number of new high priority voice messages
- Number of old high priority voice messages
- Total number of new fax messages (includes normal and high priority messages)
- Total number of old fax messages (includes normal and high priority messages)
- Number of new high priority fax messages
- Number of old high priority fax messages

Two new added APIs as CiscoAddress JTAPI extensions provide the enhanced MWI message summary information. Similar to the existing setMessageWaiting APIs, one API allows you to set the summary information for the observed address. The other API allows you to set message summary information on any address that is reachable on the observed address, as defined by the configured calling search space of the observed address.

These new APIs can also get used on phone types that do not support the enhanced message counts. If used on non-supported phones, these APIs behave similar to the existing setMessageWaiting method; that is, only the messaging waiting indicator lamp gets turned on or off, and counts do not display.

Logical Partitioning

This feature allows administrators to configure geographical locations and restrict calls that pass through a PSTN gateway to be connected directly to a VoIP phone or VoIP PSTN gateway in another geographic location. This feature allows using single-line analog phones and remains complaint with Telecom Regulatory Authority of India (TRAI) regulation.

You can turn off this feature by using the Logical Partitioning Enabled service parameter, and the feature stays disabled by default.

Component Updater

ComponentUpdater interface gets enhanced to allow applications to specify the location of updater log. Currently updater log gets created in the same directory as the application. This enhancement allows applications to specify the trace location.

Skinny Client Control Protocol (SCCP)

Enhanced Message Waiting Indication Data

The enhanced Enhanced Message Waiting (MWI) data comprise voice and fax counts. This feature enables a voice mail server to report urgent and nonurgent voice mail and fax counts to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager in turn sends the enhanced MWI data to the respective client.

Two new messages get defined. One message gets sent by the voice mail server to notify the Cisco Unified Communications Manager of the MWI data. The other message gets sent by the Cisco Unified Communications Manager in response and indicates whether the notification was successful.

H.264 Video Channel Negotiation

Because the earlier versions of the SCCP specifications were unclear about certain aspects of H.264 negotiation such as sending and receiving of frame rates below the advertised level, Release 7.1(2) added new guidelines for clients and servers to follow.

IP to IP Gateway Support

A new field that is added to the StationOpenReceiveChannelMessage carries the audio level (gain/loss) for the requested audio stream. Only the IP-IP [IOS] gateway utilizes this field.

Deprecation of Messages

StationUpdateCapabilitiesMessage and StationUpdateCapabilitiesVersion2Message get deprecated because these messages represent a subset of UpdateCapabilitiesV3Message. Therefore, clients that are compliant to SCCPv18 specification must use UpdateCapabilitiesV3Message instead. Table 1-34 lists the skinny messages that are added, modified, and deleted for Release 7.1(2).

Table 1-34 New and Updated Skinny Messages

Message Name	Status	To Cisco Unified Communications Manager	From Cisco Unified Communications Manager
StationMwiNotificationMessage	New	√	
StationMwiResponseMessage	New		√
StationStartMultiMediaTransmissionMessage	New		√
StationStartMultiMediaTransmissionAckMessage	New	√	
StationUpdateCapabilities	Deleted	√	
StationUpdateCapabilitiesVersion2	Deleted	√	
StationStartMultiMediaTransmission	Deleted		√
StationStartMultiMediaTransmissionAckMessage	Deleted	√	
StationOpenReceiveChannelMessage	Modified		√

Administrative XML (AXL) Programming

This section describes the changes that occur in Cisco Unified Communications Manager Administrative XML (AXL) APIs to support the new and updated features for the Cisco Unified Communications Manager Release 7.1(2).

H.323 Security: Voice Encryption Profile with Native H.235/H.245 Key Management

The H.235 security recommendation feature in Unified CM 7.1(2) supports the Diffie-Hellman key exchange mechanism for media encryption in a H.323 network by using procedures that are recommended in the H.235.6 Voice encryption profile with native H.235/H.245 key management standard. This feature allows the Cisco Unified Communications Manager to transparently pass the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To support this feature, the following changes occurred in the AXL API:

Table 35 Changes in AXL API to Support Media Encryption in H.323

API	Changes
H323Gateway (add/update/get)	Added an optional parameter, AllowH235PassThrough
H323Trunk (add/update/get)	Added an optional parameter, AllowH235PassThrough

IPv6 Support

Cisco Unified Communications Manager Release 7.1(2) supports IPv6 capabilities in its network. Cisco Unified Communications Manager supports IPv4 only and IPv4/IPv6 dual-stack systems. At a component level, IPv6 applies to the IP phone that is supported in dual-stack systems in the Cisco Unified Communications Manager 7.1(2).

To support this feature, the following changes occurred in the AXL API:

Table 36 Changes in AXL API to Support IPv6

API	Changes
CommonDeviceConfig (add/update/get)	Added the following optional parameters: • IPAddressingMode • IPAddressingModePreferenceControl • AllowAutoConfigurationForPhones
SIPProfile (add/update/get)	Added an optional parameter, EnableAnatForEarlyOfferCalls
SIPTrunk (add/update/get)	Added an optional parameter, destinationAddressIPv6
ProcessNode	Added an optional parameter, IPv6Name
RoutePattern	Added an optional parameter, DNOrPatternIPv6

Logical Partitioning

Cisco Unified Communications Manager Release 7.1(2) supports logical partitioning. The logical partitioning feature restricts VoIP to PSTN calls, and vice versa, based on the logical partitioning policy. Any request that interconnects a VOIP call to a PSTN call, or vice versa, in two different geographical locations fails, and the error code gets sent back to the applications.

QSIG variant Per Trunk or Gateway

A Q.SIG variant that is selectable by trunk or gateway feature allows you to configure QSIG variants on a per trunk/gateway basis.

To support this feature, the following changes occurred in the AXL API:

Table 37 Changes in AXL API to Support QSIG Variant Per Trunk or Gateway Feature

API	Changes
H323Gateway (add/update/get)	Added the following optional parameters: • ASN1ROSEOIDEncoding • QSIGVariant
H323Trunk (add/update/get)	Added the following optional parameters: • ASN1ROSEOIDEncoding • QSIGVariant
GatewayEndpoint (add/update/get)	Added the following optional parameters: • ASN1ROSEOIDEncoding • QSIGVariant
MGCPEndpoint (add/update/get)	Added the following optional parameters: • ASN1ROSEOIDEncoding • QSIGVariant

Enhancements to Calling Party Number Transformations

The Calling Party Number (CPN) enhancement feature enhances Cisco Unified Communications Manager system capability to provide accurate calling party number information to the phones. Cisco Unified CM DB/Administrator gets enhanced to allow configuration of transformation CSS for each calling party number type (National, International, Unknown, Subscriber) on the gateway, trunk, and device pool configuration windows. This gives Cisco Unified CM the ability to conditionally transform the calling party number based on the number type. Also, an option that is provided in Cisco Unified CM administrator allows you to configure Number of Digits to Strip for each number type in addition to the already available Prefix fields. This replaces the colon (:) notation that was added in earlier releases. You can do this only at the device/device-pool level. At the service parameter level, the existing colon (:) notation remains.

Barge Enhancement Feature

Party Entrance Tone configuration gets provided on a per-line basis, rather than per-cluster basis. This Party Entrance Tone gets used for barge, cBarge, ad hoc conference, join, and meet-me conference.

To support this feature, an optional parameter, partyEntranceTone, now exists in the Line (add/update/get) API.

Enhanced Clear Channel (G.clear) Support

The enhanced Clear Channel feature enhances sRTP support for a Clear Channel (G.Clear) data call between MGCP, SIP line, and SIP trunk. H323 endpoint does not get included in this feature.

Prior to this feature, Cisco Unified Communications Manager only supported non-secured G.Clear call. G.Clear call over SIP interface requires early offer. For MGCP-to-SIP interoperability, no sRTP key gets provided to exchange for early offer call. With this feature, the RSVP layer generates a fake key for the SDP in the outgoing INVITE if this is sRTP call for G.Clear early offer call.

To support this feature, an optional parameter, gClear, now exists in the SIPProfile (add/update/get) API.

Always Use Prime Line

The Always Use Prime line feature enables a user to always answer on prime line upon off hook. The Always Use Prime Line for voice message capability enables user to always access a voice message on prime line when messages button is pressed. This feature previously got supported at the system level. Current enhancement provides control at the device level, which enables the individual device/user to control.

To support this feature, the following changes occurred in the AXL API:

Table 1-38 Changes in AXL API to Support Enhanced Clear Channel

API	Changes
Phone (add/update/get)	Added the following optional parameters: • alwaysUsePrimeLine • alwaysUsePrimeLineforVoiceMessage
CommonPhoneConfig (add/update/get)	For this new API. as part of this feature, the following optional parameters get added to this API: • alwaysUsePrimeLine • alwaysUsePrimeLineforVoiceMessage
DeviceProfile	Added the following optional parameters: • alwaysUsePrimeLine • alwaysUsePrimeLineforVoiceMessage

SSH Userid and Password Configured in the Common Phone Profile

Before Release 7.1(2), you configured SSH credentials in the device window, and that made it time-consuming to configure credentials for a large number of phones. This feature enables configuring once in the Common Phone Profile that enables SSH credentials in a group of phones.

To support this feature, Release 7.1(2) adds a new API, CommonPhoneConfig (add/update/get), with the following optional parameters:

- sshUserId
- sshPwd

Serviceability XML Programming

This section describes the changes that were made in the Cisco Unified Communications Manager Serviceability APIs to support the new and updated features for Cisco Unified Communications Manager Release 7.1(2).

IPv6 Support

Cisco Unified Communications Manager Release 7.1(2) supports IPv6 capabilities in its network. Cisco Unified Communications Manager supports IPv4 only and IPv4/IPv6 dual-stack systems. At the component level, IPv6 only applies to IP phones that are supported in dual-stack systems in Release 7.1(2).

To support this feature, the following changes occurred in the Serviceability APIs:

- Added a new API, SelectCmDevice, to display IPv6 details of Cisco Unified Communications Manager node or server, phone devices, SIP devices, and media devices.
- Added a new API, SelectCtiDevice, to support IPv6 address search for CTI-controlled application and devices.
- The following performance monitoring counters show the IPv6 network statistics:
  - In Receives
  - In HdrErrors
  - In UnknownProtos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reads
  - Reasm OKs
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- CISCO-CCM-MIB enhancement shows IPv6 details of Cisco Unified Communications Manager node, phone devices, SIP devices, and media devices.

Seamless Upgrade

Seamless Upgrade represents the ability of phones to download a new firmware image in the background while phones remain in service.

To support this feature, the Serviceability APIs optionally provide the following information per device:

- Phone Active Load ID
- Phone InActive Load ID
- Phone Down Load Status
- Phone Down Load Failure Reason
- Phone Firmware Down Loaded Server

Cisco Unified IP Phones

This section provides information for the following features:

- Barge Tone Enhancements, page 185
- Cisco Unified IP Phone Support HTTPS, page 186
- Hold Status, page 186
- Internet Protocol Version 6 on the Cisco Unified IP Phone, page 187

- Line Select, page 188
- Missed Calls, page 189
- Off-Hook Abbreviated Dial, page 122
- Restrict Unconfigured Phone Registration, page 190
- Secure Icon, page 191
- Cisco Web Dialer Enhancements, page 192

Barge Tone Enhancements

Be aware that the Party Entrance Tone configuration is available as a per-line setting, in addition to a service parameter setting for Cisco Unified CM administrators. The default value for the line setting specifies the service parameter setting. The Party Entrance Tone setting gets applied to barge, cBarge, join, ad hoc, and meet-me conferences. For more information, see the "Party Entrance Tone" section on page 125.

Barge and cBarge support the interaction with Private Line Automatic Ringdown (PLAR). When a shared line has PLAR configured, a user can Barge or cBarge into a call that is connected on the shared PLAR line.

These Barge Tone enhancements get supported on the following phones that are running SIP and SCCP:

- 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 Guide*
- *Cisco Unified IP Phone Administration Guide*
- Barge, cBarge, and Single Button Barge Support for PLAR, page 39
- Party Entrance Tone, page 125

Cisco Unified IP Phone Support HTTPS

Cisco Unified IP Phones can securely access the web with the use of a phone trust store that is called "phone-trust." Administrators can upload certificates to a phone-trust store by using the Cisco Unified Communications Manager Operating System GUI. The Cisco Unified IP Phone will display a menu option called "Application Server" for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Cisco Unified IP Phone CTL file.

The phone-trust certificates and secure HTTPS web access get supported on the following phones that are running SIP and SCCP:

- 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 Operating System Administration Guide*
- *Cisco Unified Communication Manager Security Guide*

Hold Status

Cisco Unified Communications Manager 6.1(3) and 7.1(2) introduced the following enhancements to hold status:

- The Hold Status feature allows phones with a shared line to distinguish whether the local user placed the call on hold or a remote (shared line) user placed the call on hold.
- If two phone users share a line and one user places a call on hold, that user phone displays the local hold icon while the other user phone displays the remote hold icon. In addition, on the Cisco Unified IP Phone 7906G and 7911G, the hold button stays solid red on the local and remote phone. On all other supported phones, the local phone LED flashes green, and the remote phone user LED flashes green.

The hold status enhancement gets supported on the following phones that are running SIP and SCCP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G

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

Where to Find More Information

- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*
- Viewing Held Calls on Shared Lines, page 140

Internet Protocol Version 6 on the Cisco Unified IP Phone

For more information on using Internet Protocol Version 6 on the Cisco Unified IP Phone, see the "Phone Considerations" section on page 85.

The following phones that are running SCCP support IPv6:

- 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

For More Information

- "Internet Protocol Version 6 (IPv6)," *Cisco Unified Communications Manager Features and Services Guide*
- Phone Considerations, page 85
- Internet Protocol Version 6 (IPv6), page 64

Line Select

Cisco Unified Communications Manager 6.1(3) and 7.1(2) introduced settings to determine whether the primary line gets automatically selected when a call is answered or when the Messages button gets pressed. You can configure these settings for all phones in the system, or for a single phone.

- **Line Select (Always use Prime line)**—If this feature is disabled (default), the ringing line gets selected. When feature is enabled, the primary line gets picked up even if a call is ringing on another line. The user must manually select the other line.
- **Line Select for Voice Messages (Always use Prime line for Voice Message)**—When this setting is disabled (default), pressing the Messages button connects to the line that has a voice message. If more than one line has voice mail, the first available line gets selected. When setting is enabled, the primary line always gets used to retrieve voice messages.

Note Be aware that the primary line settings are also available for phones that are using Cisco Extension Mobility.

These enhancements get supported on the following phones that are running SCCP or 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

Where to Find More Information

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

Missed Calls

The Missed Calls feature allows the phone administrator to specify whether missed calls will get logged in the missed calls directory for a given line appearance. The following properties apply to the missed calls feature:

- The line can act as a directory number or shared line. The default behavior logs all missed calls on all lines.
- Missed call logging operates on a line basis. The line can act as a directory number or a shared line.
- If the administrator configures a line appearance (share or non-shared), so missed calls do not get logged, calls to that line never get logged in the missed call log directory, even if the calls eventually get forwarded due to no answer.
- If more than one line key gets configured on a phone, logging missed calls depends on the missed call log setting for each line.
- An on/off configuration parameter that is sent to the phone in the configuration file controls the missed calls logging.
- The missed calls log configuration does not affect any existing or previous call log items.
- Calls on lines that are not logged do not affect the New Missed Call status message.
- If the phone administrator turns off the missed calls feature on the configured line appearance, the missed calls do not get listed in the missed call history on that line appearance.

In addition to these properties, the following properties continue to apply to all calls:

- All calls that are received on a phone display in the Received Calls log, regardless of the line on which they were received.
- All calls that are made from a phone display in the Placed Calls log, regardless of whether they were placed from a shared or primary line.

The missed calls feature gets supported on the following phones that are running SCCP or SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

- *Cisco Unified IP Phone Administration Guide*

Off-Hook Abbreviated Dialing

Cisco Unified Communications Manager Release 7.1(2) introduces the Off-Hook Abbreviated Dialing feature. The user can initiate off-hook abbreviated dialing while user is conferencing a call, while user is transferring a call, or while user is placing a new call after putting a call on hold.

Cisco Unified Communications Manager Configuration Tips

- Assign the softkey, **AbbrDial**, to the phone by using Softkey Template Configuration. The following phone states apply: Offhook, Offhook with Feature, and Digits After First.

The Off-Hook Abbreviated Dialing feature gets supported on the following phones that are running SCCP or 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

For More Information

- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Softkey Template Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*

Restrict Unconfigured Phone Registration

In Cisco Unified Communications Manager releases other than 6.1(3) and 7.1(2), if a Cisco Unified IP Phone had not been added to the Cisco Unified Communications Manager database and did not have autoregistration enabled, the phone would repeatedly attempt to register (unsuccessfully) with Cisco Unified Communications Manager, thus continually notifying Cisco Unified Communications Manager with these repeated registration requests.

With Cisco Unified Communications Manager Releases 6.1(3) and 7.1(2), if autoregistration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager. The phone continues to display the "Configuring IP" message until autoregistration is enabled or until the phone has been added to the Cisco Unified Communications Manager database.

The registration behavior gets supported on the following devices or phones that are running SIP or SCCP:

- 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
- VG248 Gateways

Where to Find More Information

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

Secure Icon

Cisco Unified Communications Manager Release 7.1(2) uses a different method to calculate which Security icon to send to Cisco Unified IP Phones. Prior to release 7.1(2), the audio stream that was involved in a call or conference provided the sole basis for the type of security icon that Cisco Unified Communications Manager sent to phones. However, in Cisco Unified Communications Manager Release 7.1(2), Cisco Unified Communications Manager calculates which security icon to display based on both audio and video (if applicable) streams, and sends the resulting security icon to the Cisco Unified IP Phone.

All media that are involved in the call must be secure for the Lock (Encrypted) icon to display on the phone. For example, if the audio is encrypted but the video is not encrypted, the security icon that displays does not represent the Lock (Encrypted) icon because the call as a whole is not encrypted. Instead, the Shield (Authenticated) icon, if one exists for the given phone model, displays on the phone. For phones that do not support Shield icons, these phones will not display any security icon for an Authenticated call or conference.

For a table that shows which type of security icon to expect for various call scenarios, refer to the *Cisco Unified Communications Manager Security Guide,* "Security Icons" section.

New Behavior for Secure-Tone Feature

In releases prior to Cisco Unified Communications Manager Release 7.1(2), a security tone would play to indicate that a call was “protected,” which meant that two phones on a call were configured for Protected mode and that the phones were receiving and transmitting encrypted audio. Beginning with Cisco Unified Communications Manager Release 7.1(2), if a video stream is also involved in the call, the security tone will play only if both phones are receiving and transmitting encrypted video as well as encrypted audio.

The secure icon feature gets supported on the following phones that run SCCP or 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

For More Information

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

Cisco Web Dialer Enhancements

Cisco Unified Communications Manager supports the following Cisco Web Dialer enhancements:

- Changing the Cisco Web Dialer Database Location—The list of Cisco Web Dialers moved from the Service Parameter Configuration window in Cisco Unified Communications Manager Administration to be node-specific in the Application Server Configuration window. The Application Server Configuration window get updated to enable sorting by application server type and node.

  For more information on this topic, see the “Cisco Web Dialer Configured in Application Server Window” section on page 49.
- Preferred Device Menu Name Change—In the Cisco WebDialer Make Call window, the “Use permanent device” changed to display “Use preferred device”. When only one preferred device is available, the MAC address does not display in the menu. MAC addresses will only display if two or more devices of the same type are assigned to the user.
- Merging the Preferences and Make Call Windows Together—The Cisco WebDialer Preferences window options now display in the Cisco WebDialer Make Call window.

- Integration with Extension Mobility—If the user has an Extension Mobility profile, you can access an option that is labeled “Use my Extension Mobility logged in device” from the Preferred Device menu.
- Dialog changes for Hang-Up UI—The text on the Hang-Up UI changes:

  Calling <Username if available> at <dial-out number>

  If authorization codes are required, enter them now

The Cisco Web Dialer enhancements get supported on the following phones that are running SIP or SCCP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

Table 39 lists Cisco Unified IP Phones that support new Cisco Unified Communications Manager features.

Table 39 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Barge Tone Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Barge Tone Enhancements, page 185

Table 39 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Cisco Unified IP Phone Support HTTPS	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Cisco Unified IP Phone Support HTTPS, page 186
Hold Status	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Hold Status, page 186
Internet Protocol Version 6 (IPv6)	SCCP only 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931 7911G 7906G	

Table 39 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Line Select	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Line Select, page 188
Missed Calls	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Missed Calls, page 189
Off Hook Abbreviated Dialing	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Off-Hook Abbreviated Dialing, page 190

Table 39 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Restrict Unconfigured Phone Registration	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Restrict Unconfigured Phone Registration, page 190
Secure Icon	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Secure Icon, page 191
Cisco Web Dialer Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Cisco Web Dialer Enhancements, page 192

Cisco Unified CM User Options

See the following sections for enhancements to the Cisco Unified CM User Options:

- Logging Missed Calls for Shared Lines, page 107
- Cisco Web Dialer Enhancements, page 192

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(2) As of May 27, 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(2) As of May 27, 2009" section on page 199 to access the online record for that defect, including workarounds.

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

When you open the online record for a defect, you will see data in the "First Fixed-in Version" field. The information that displays in this field identifies the list of Cisco Unified Communications Manager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Communications Manager releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1. However, the version information that displays for the Cisco Unified Communications Manager maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco Unified Communications Manager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

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

Note Because defect status continually changes, be aware that the "Open Caveats for Cisco Unified Communications Manager Release 7.1(2) As of May 27, 2009" section on page 199 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 197.

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(2) As of May 27, 2009

The following information comprises unexpected behavior (as of May 27, 2009) that you may encounter in Release 7.1(2) of Cisco Unified Communications Manager.

BPS BAT

- CSCsz79330 Job status displays as Incomplete in Job Scheduler window.

CAR

- CSCsz77936 The need exists for individual bill summary report enhancements.
- CSCsz81637 File ownership in the /car folder changes after upgrade.

CM Serviceability

- CSCsz17512 Network disruptions cause CEF core dump.

CMCTI

- CSCsz43575 Application can open unregistered line if it is not CTI controllable.
- CSCsr30432 Click to Conference: Unified CM fails to send NOTIFY.
- CSCsr94857 CTIManager IMS needs change notification when LDAP server gets updated.
- CSCsu08818 CTI Manager crashed during upgrade.
- CSCsw36765 CTI sends the Device State Event even though DND option is set to reject.
- CSCsz56287 The needs exists for CTI to handle unsupported characters or digits in the dial string.

CMUI

- CSCsz25352 Unified CM OS cannot ping if an upgrade is in progress. CLI ping does work.
- CSCsz20821 Entry added on Fast Dial window shows 0 records found.
- CSCsz13707 Serviceability PSC config item cannot be changed on Standard Common Phone Profile.
- CSCsz48205 When the DPark number gets updated to range, BLF key should not get updated.
- CSCsz62409 Switch versions hang in cmplatform in browser webapp.
- CSCsz43236 Bulk migration phone search returns incorrect results
- CSCsz85446 Phone button template does not display in the Find List window after it got added successfully.

CP-CAC

- CSCsu88429 Bandwidth gets partially reserved when call that originated from a specific branch gets connected to a VXML gateway on a separate branch that is using the SIP or H.323 trunk.

CP-ChangeNotify

- CSCsz46502 Update of partition name causes RNA to fail.

CP-H323

- CSCsz19793 At the end of a conference call, the last party receives reorder tone instead of normal clearing.
- CSCsz91530 Conferencing does not work when multiple H323 gateways get added in RG with LP enabled.

CP-LineControl

- CSCsu91271 Delayed media setup occurs with a shared DN (43 phones).

CP-MediaControl

- CSCsy95581 Resume fails over SIP trunk on incorrect codec for MTP/xcoder selection.
- CSCsu91093 IPV6: After a transfer, no video exists on Cisco Unified Personal Communicator and Cisco Unified Video Advantage.
- CSCsy00728 Hold/Resume seems broken for some dual-stack intercluster video calls.
- CSCsy81095 Wrong CAC bandwidth gets allocated for IPv6 calls with SIP trunk and MTP/X.
- CSCsz53861 Consult transfer failure occurs with SIP-encrypted endpoint over SIP TLS.
- CSCsy62649 Call drops after a sequence of blind and supervised transfers through a tandem cluster with SIPICT, H323ICT, IPV6, and sRTP involved.
- CSCsy72140 Secured call that gets blind transferred across SIP trunks with H.323 ICT experiences 2-way audio after hold and resume.

CP-PRI

- CSCsz76370 Unified CM cannot relay calling name within subsequent facility message.

CP-SCCP

- CSCsw80362 Resume held call on customer phone fails during recording.

CP-SIP Trunk

- CSCsz42217 Calls fail to transfer from Unity Connection via SIP trunk.
- CSCsu95169 Call over SIP trunk and H323t cannot join meet-me conference.

CP-System

- CSCsz14019 Core dump occurs during load run.
- CSCsz73088 Unified CM publisher server virtual memory usage increased 20 percent.

CPI AppInstall

- CSCsz59824 Upgrade fails for SFTP/FTP/DVD.

CPI Diagnose

- CSCsz32585 /var/log/active/platform/log/diag4.log is incorrect.

CPI OS

- CSCsz23430 IBM ServeRAID 8k/8k-1 takes too long to boot.

- CSCsz70804 IBM x3650M2 uEFI firmware and setup fail with DVD install.
- CSCsz85521 After switchback from Unified CM 7.1.2 to Unified CM 5.1.3, DVD cannot be read.

CPI Platform API

- CSCsz26525 When server downloads a load, OS GUI Settings > Version does not work. CLI can restart, switch version, and shut down.
- CSCsz41104 When server downloads a load, DHCP setting OS GUI does not work, but CLI does.

CPI Security

- CSCsl81015 Intermittent alert displays in RTMT.
- CSCsz59746 CLI "file delete" command should not cause informixauditlog files to be deleted.
- CSCsz79892 Invalid source address does not get flagged in Unified CM IPSec configuration.

Database

- CSCsz48237 Plus dialing digit (+) for international numbering plans does not work as a Directed CallPark prefix digit.
- CSCsz80490 DMA failed.
- CSCsz80761 Database restore_uff process does not report the correct dbreplication.
- CSCsz09666 Dbmon database connections increase due to an odbc hang.

Database IDS

- CSCsy52717 Replication shuts down without warning.
- CSCsz46109 Database stays inaccessible from subscriber servers, and services remain in "Starting" status.
- CSCsr41156 After user reboots firewall between Unified CM nodes, service core occurs.

JTAPI SDK

- CSCsv28679 CallCtlTermConnBridgedEv on shared lines occurs with different cause NORMAL.
- CSCsx68090 Synchronous CallObservationEndedEv on redirect does not occur.
- CSCsx65635 CallCtlTermConnDroppedEv occurs with CAUSE_TRANSFER.
- CSCsy91652 Parking a call in a conference does not trigger ConnDisconnected.

RISDC

- CSCsz55947 RisDC core dump occurs during upgrade.

RTMT

- CSCsv95745 Create directory button gets disabled

Voice SIPstack

- CSCsz77128 If session target that is configured exceeds 32 bytes, memory corruption can occur.

Documentation Updates

This section contains information on documentation omissions, errors, and updates for the following Release 7.1(2) documentation:

- Cisco Unified Communication Manager CDR Analysis and Reporting, page 202
- Cisco Unified Communications Manager Security, page 202
- Cisco Unified Communications Operating System, page 204
- Cisco Unified Communications Manager Administration, page 205
- Cisco Unified Serviceability, page 212

Cisco Unified Communication Manager CDR Analysis and Reporting

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

- Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting, page 202
- "Mailing a Report" Recipients, page 202

Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting

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

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

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

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

"Mailing a Report" Recipients

The "Mailing a Report" chapter in the CDR Analysis and Reporting Administration Guide omits this information:

When the Mailing option gets enabled,

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

Cisco Unified Communications Manager Security

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

Definition of Locally Significant Certificate

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

Using Certificates Issued by a Third-Party Certificate Authority

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

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

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

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

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

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

Cisco Unified Communications Operating System

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

- Guidelines for Installing COP Files, page 204
- Disk Space Before Upgrading, page 204
- Pre-Upgrade Task Is Omitted From Software Upgrades Chapter, page 205

Guidelines for Installing COP Files

The following guidelines apply to installing COP files. If the documentation for a specific COP file contradicts these general guidelines, follow the COP file documentation:

- Install the COP file on every server in a cluster.
- After you install a COP file, you should restart the server.

  This restart ensures that configuration changes that are made during the COP file installation get written into the database. Cisco recommends that you perform this restart during an off-peak period.

Disk Space Before Upgrading

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

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

- Use the **show status** CLI command and note the information that displays under the Disk/logging heading.
- From Cisco Unified Communications Operating System, choose **Show > System**.
- From Cisco Unified Real-Time Monitoring Tool, choose **System > Server > Disk Usage**. Choose the server from the Disk Usage at Host drop-down list box and view the Used Space (MB) for the Common partition.

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

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

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

Pre-Upgrade Task Is Omitted From Software Upgrades Chapter

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

Before you perform the Cisco Unified Communications Manager 7.1(2) upgrade, ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.

Cisco Unified Communications Manager Administration

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

- Number of Locations and Regions That Cisco Unified Communications Manager Supports, page 206
- Intercom Route Partition Configuration Settings Description Field Information Is Incorrect, page 206
- Mobile Connect Support Restrictions, page 206
- Configuring an H.323 Gateway for System Remote Access by Using Hairpinning, page 206
- Enterprise Feature Access Two-Stage Dialing, page 207
- Valid Characters in Name Field of Access List Configuration Window, page 207
- Valid Characters in Name Field of Role Configuration Window, page 207
- Valid Characters in Name and Description Fields of Remote Destination Profile Window, page 207
- Valid Characters in Name Field of Geolocation Filter Configuration Window, page 208
- Valid Characters in Name Field of Geolocation Configuration Window, page 208
- IPv6 Chapter Incorrectly Describes How IPv6 Addresses Display in the Find and List Phones Window, page 208
- Directory Number Chapter Includes Incorrect Information on Alerting Name and Display Name Fields, page 209
- End User Chapter Includes Incorrect Information for Manager User ID Field, page 210
- Intercom Calls Cannot Be Placed on Hold, page 210
- Device Pool Configuration Chapter Does Not State That You Can Enter -1 in the Connection Monitor Duration Field, page 210
- Trunk Configuration Chapter Does Not State That You Can Enter Hostname in Destination Address Field, page 210
- IPv6 Chapter Does Not Contain Information on NTP Server, page 211
- Licensing Chapter Does Not State That You Should Use Microsoft Outlook to Receive Licenses, page 211
- Voice Mail Chapters Do Not Describe MWI Service Parameter, page 211
- Cisco Unified Communications Manager Does Not Support Logical Partitioning for Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express Calls, page 212

- Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters, page 212
- Mobile Voice Access Directory Number Field Description, page 212
- Recording Destination Address Field Description, page 212
- OpenLDAP Version 2.3.41 Not Listed in LDAP Synchronization Documentation, page 212

Number of Locations and Regions That Cisco Unified Communications Manager Supports

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

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

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

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

Intercom Route Partition Configuration Settings Description Field Information Is Incorrect

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

Mobile Connect Support Restrictions

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

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

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

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

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

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

Enterprise Feature Access Two-Stage Dialing

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

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

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

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

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

Valid Characters in Name Field of Access List Configuration Window

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

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

Valid Characters in Name Field of Role Configuration Window

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

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

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

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

Name

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

Description

Enter a text description of the remote destination profile.

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

Valid Characters in Name Field of Geolocation Filter Configuration Window

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

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

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

Valid Characters in Name Field of Geolocation Configuration Window

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

Enter a unique name for this geolocation.

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

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

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

Incorrect Information

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

Correct Information

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

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

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

Incorrect Information

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

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

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

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

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

Correct Information

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

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

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

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

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

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

End User Chapter Includes Incorrect Information for Manager User ID Field

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

Incorrect Description

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

Correct Description

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

Intercom Calls Cannot Be Placed on Hold

The Restrictions section of the “Intercom” chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly indicates that intercom calls can be placed on hold. Actually, intercom calls cannot be placed on hold.

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

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

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

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

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

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

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

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

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

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

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

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

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

IPv6 Chapter Does Not Contain Information on NTP Server

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

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

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

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

The following document omits this limitation:

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

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

The "Licensing" chapter in the *Cisco Unified Communications Manager System Guide* does not state that Cisco recommends that you use Microsoft Outlook when you receive Cisco Unified Communications Manager licenses. For more information on this topic, see the "Use Microsoft Outlook to Receive Cisco Unified Communications Manager Licenses" section on page 16.

Voice Mail Chapters Do Not Describe MWI Service Parameter

The voice mail chapters in the *Cisco Unified Communications Manager System Guide* do not describe the Multiple Tenant MWI Modes service parameter. For information on this service parameter, see the "Multiple Tenant MWI Modes Service Parameter" section on page 16.

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

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

The following document omits this limitation:

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

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

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

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

Mobile Voice Access Directory Number Field Description

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

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

Recording Destination Address Field Description

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

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

OpenLDAP Version 2.3.41 Not Listed in LDAP Synchronization Documentation

The “Understanding the Directory” chapter in the *Cisco Unified Communications Manager System Guide* does not state the version of OpenLDAP that is supported for LDAP Synchronization with Cisco Unified Communications Manager Release 7.1(2). To identify the supported version, see the OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database, page 125.

Cisco Unified Serviceability

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

- Password Description Omitted, page 213

- Cluster Service Activation Node Recommendations, page 213

Password Description Omitted

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

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

Cluster Service Activation Node Recommendations

The “Configuring Services” chapter in the *Cisco Unified Serviceability Administration Guide* does not include the following information that describes service activation recommendations for specific nodes in a cluster. Table 40 provides a general summary of the cluster activation recommendations for a feature service in these nodes: publisher, subscriber, TFTP, and MOH. For specific recommendations that are associated with activating a particular feature service, refer to the Cluster Service Activation Recommendations section in the “Configuring Services” chapter.

Table 40 Cluster Service Activation Node Recommendations

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager	Deactivated	**Activated**	Deactivated	Deactivated	
Cisco TFTP	Deactivated	Deactivated	**Activated**	Deactivated	
Cisco Messaging Interface	Deactivated	Deactivated	Deactivated	Deactivated	Do not activate this service if you plan to use Cisco Unity voice-messaging system.
Cisco Unified Mobile Voice Access Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use this application, activate this service on the first node only.
Cisco IP Voice Media Streaming App	Deactivated	Deactivated	Deactivated	**Activated**	Do not activate this service on the first node or on any nodes that run the Cisco CallManager service.
Cisco CTIManager	Deactivated	**Activated**	Deactivated	Deactivated	Activate this service on each subscriber node to which JTAPI/TAPI applications will connect.
Cisco Extension Mobility	Deactivated	**Optional**	Deactivated	Deactivated	If you use EM, activate this service on all subscriber nodes in the cluster.
Cisco Extended Functions	Deactivated	**Optional**	Deactivated	Deactivated	If you use extended functions, activate this service on one or more servers.
Cisco Dialed Number Analyzer	Deactivated	**Optional**	Deactivated	Deactivated	If you need DHCP service, activate this service on the node with the least amount of call-processing activity.
Cisco DHCP Monitor Service	Deactivated	Deactivated	Deactivated	Deactivated	Activate this service on the node that has DHCP enabled.

Table 40 Cluster Service Activation Node Recommendations (continued)

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager Attendant Console Server	Deactivated	**Optional**	Deactivated	Deactivated	To use Cisco Unified Communications Manager Attendant Console, activate this service on every subscriber node in the cluster that runs the Cisco CallManager service.
Cisco IP Manager Assistant	Deactivated	**Optional**	Deactivated	Deactivated	If you use IPMA, activate this service on any subscriber nodes (primary and backup - up to six servers for three pairs maximum) in the cluster.
Cisco Web Dialer Web Service	Deactivated	**Optional**	Deactivated	Deactivated	If you use Web Dialer, activate this service on one or more subscriber node(s).
Cisco SOAP-CDROnDemand Service	**Optional**	Deactivated	Deactivated	Deactivated	If you want to collect CDR files by using SOAP, activate the service on the first node only.
Cisco CAR Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAR, activate this service on the first node only.
Cisco AXL Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you need this service, activate the service on the first node only.
Cisco Bulk Provisioning Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use BAT, activate the service on the first node only.
Cisco TAPS Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use TAPS, activate the service on the first node only.
Cisco Serviceability Reporter	**Activated**	Deactivated	Deactivated	Deactivated	Activate this service on the first node only.
Cisco CallManager SNMP Service	**Activated**	**Activated**	**Activated**	**Activated**	If you use SNMP, activate this service on all servers in the cluster (optional, but activation recommended).
Cisco CTL Provider	**Optional**	**Optional**	**Optional**	**Optional**	If you use CTL, activate this service on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAPF, activate this service on the first node only.
Cisco DirSync	**Optional**	Deactivated	Deactivated	Deactivated	If you use DirSync, activate this service on the first node only.

Activated = activated at installation

Optional = activate only if the application is needed

Obtaining Documentation and Submitting a Service Request

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

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

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