Release Notes for Cisco Unified Communications Manager Release 6.0(1a)

August 3, 2007

These release notes describe updates and caveats for Cisco Unified Communications Manager Release 6.0(1a). 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 4 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 must upgrade to Cisco Unified Communications Manager 6.0(1a).

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the "Upgrading System Software" section on page 2.

Contents

These release notes discuss the following topics:

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

Introduction

Cisco Unified Communications Manager, a network business communication system, provides high-quality telephony over IP networks. Cisco Unified Communications Manager enables the conversion of conventional, proprietary, circuit-switched PBXs to multiservice, open LAN systems.

System Requirements

Make sure that you install and configure Cisco Unified Communications Manager Release 6.0(1x) on a Cisco Media Convergence Server (MCS).

You may also install Cisco Unified Communications Manager on a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

Cisco Unified Communications Manager requires a minimum of the following items on the Cisco MCS.

- 2 GB of memory
- 72 GB disk drive
- 2 GHz processor

Supported Platforms

To find which servers support the Cisco Unified Communications Manager Release 6.0(1x), refer to the *Cisco Unified Communications Manager Server Support Matrix* at http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html

Note Cisco recommends that you connect each Cisco Unified Communications node to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure. See the "Basic Uninterruptible Power Supply (UPS) Integration" section on page 12

Determining the Software Version

To determine the software version of Cisco Unified Communications Manager, open Cisco Unified Communications Manager Administration. The following information displays:

- Cisco Unified Communications Manager System version
- Cisco Unified Communications Manager Administration version

Upgrading System Software

You can access the latest software upgrades for Cisco Unified Communications Manager 6.0(x1) on Cisco.com. Table 1 lists the URLs from which you download the software.

Warning **If you are upgrading from an Engineering Special (ES) on an earlier version of Cisco Unified Communications Manager to this version you may lose fixes. Any ES produced within a 30 day period prior to release of this upgrade may contain fixes not included in this release. Please ensure that any critical defect for which you deployed an ES is also included in this upgrade.**

Table 1 Download URLs for Software Upgrades

Software	Download URL
Cisco Unified Communications Manager 6.0(1x)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-60
Locale installers	http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml
Phone firmware	http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto
Cisco Security Agent (CSA)	http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des
Upgrade Assistant	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-utilpage

Related Documentation

The documentation that supports Cisco Unified Communications Manager Release 6.0(1x) resides at: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Limitations and Restrictions

A recommendation of compatible software releases that have been verified by the test for customers represents a major deliverable of the Cisco Unified Communications 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 that were tested for interoperability with Cisco Unified Communications Manager 6.0(1x) as part of Unified Communications System Release 6.0(1x) testing, see http://www.cisco.com/go/unified-techinfo.

For a list of software and firmware versions of contact center components that were tested for interoperability with Cisco Unified Communications Manager 6.0(1) as part of Unified Communications System Release 6.0(1x) testing, see http://tools.cisco.com/ITDIT/vtgsca/.

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 Communications Manager, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified Communications Manager 6.0(1x). For the most current compatibility combinations and defects that are associated with other Cisco Unified Communications 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 6.0(1x).

Important Notes for Cisco Unified Communications Manager Release 6.0(1a)

Important Notes for Cisco Unified Communications Manager Release 6.0(1)

CSCsi75567 MCS-7825H2-IPC1 Reboots Randomly

Sporadic reboots of the 7825H2 servers get triggered during long system hangs. ASR functionality autorecovers the servers after 10 minutes of kernel unresponsiveness. Event timing ranges from once every 3 months to once every 3 days.

Workaround

See http://www.cisco.com/warp/public/770/fn62850.shtml.

New Clustering Over WAN Requirements

Every 10,000 busy hour call attempts (BHCA) between sites that are clustered over the WAN requires 900kbps of bandwidth for Intra-Cluster Communication Signalling (ICCS). This is a minimum bandwidth requirement for call control traffic and is classified as priority traffic. Additional ICCS bandwidth should be allocated at 900Kbps per 10,000 BHCA.

The minimum recommended bandwidth between sites that are clustered over the WAN is 1.544Mbps. This amount allows for the minimum of 900kbps for ICCS and 644kbps for database and other inter-server traffic.

In prior versions of Cisco Unified Communications Manager, subscriber servers in the cluster use the publisher database for READ/WRITE access, and only use the local database for READ access when the publisher database cannot be reached. With Cisco Unified Communications Manager Release 6.0, subscriber servers in the cluster READ the local database. DB WRITES happens in both the local database as well as the publisher database, depending on the type of data. DBMS (IDS) replication is used to synchronize the databases on the nodes of the cluster. When recovering from a failover conditions such as loss of WAN connectivity for extended period of time, the Cisco Unified Communications Manager databases need to be synchronized with any changes that may have been made during the outage. This process happens automatically when database connectivity gets restored. This process may take longer over low bandwidth and/or higher delay links.

DB REPLICATION REPAIR/RESET:

At some point, resetting or repairing database replication between the Cisco Unified Communications Manager servers may be required. To do this, use the **utils dbreplication repair all** or **utils dbreplication reset all** command at the command line interface (CLI).

Repairing or resetting database replication using the CLI on remote subscribers over the WAN causes all Cisco Unified Communications Manager databases in the cluster to be re-synchronized, requiring additional bandwidth above 1.544 Mbps. Database replication over lower bandwidths may take longer.

Note Repairing or resetting database replication on multiple subscribers at the same remote location may take longer to complete. Cisco recommends repairing or resetting database replication of these remote subscribers one at a time.

Repairing or resetting database replication on multiple subscribers at different remote locations can occur simultaneously.

Voice, Cisco Fax Relay and Fax Passthrough Calls Fail

Voice, Cisco Fax Relay and Fax Passthrough calls fail when **mgcp fax t38 inhibit** command is configured.

Workaround

When you disable T.38 fax relay, you should also disable fxr-package (which is enabled by default) and reset the MGCP service.

Note If the gateway and call agent fail on the fax protocol negotiation, all calls get rejected, including voice calls.

Device Reset Speed

You might notice that phone device reset takes longer than in previous releases, especially in large scale clusters.

Workaround

To mitigate the decrease in speed, Cisco recommends that customers with more than 1000 users on a system wait until the maintenance window to perform a device reset on the phones.

No Such Name Error Returned in the SNMP Response

If the getbulk/getnext/getmany request contains multiple OID variables in its request PDU and the subsequent tables appear empty in the CISCO-CCM MIB, the responses may include NO_SUCH_NAME, for SNMP v1 version or GENERIC_ERROR, for SNMP v2c or v3 version because the amount of time it takes to process the SNMP requests exceeds the MasterAgent timeout duration (currently set at 25 seconds).

Workaround

You can do many things to avoid this problem, including the following workaround:

- Use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine the table size before you access the table or perform the **get** operation on the desired table first and then query the non-empty tables.
- Reduce the number of variables that are queried in a single request. For example, if the management application specifies timeout at 3 seconds for empty tables, Cisco recommends that you specify no more than 1 OID. For non-empty tables it takes 1 second to retrieve one row of data.
- Increase the response timeout.
- Reduce the number of retries.
- Do not use getbulk SNMP API. Getbulk API gets the number of records that is specified by MaxRepitions. This means that even if the next object goes outside the table or MIB, it gets those objects. So if the Cisco Unified Communications Manager MIB has empty tables, it goes to next MIB and so will require more time to respond. When you know that the table is not empty, use getbulk API. Under these conditions, limit the maximum repetition counts to 5 to get a response within 5 seconds.
- Structure SNMP queries to reflect current limits.

Note The SNMP standard requires that getnext and getbulk APIs return the next available object even if the end of the table has been reached. In the case of empty tables, the CCMAgent keeps traversing the MIB tree until it finds data to return.

Value of the Maximum Current Requests Service Parameter After Upgrade to Release 6.0

The Cisco Extension Mobility service parameter, Maximum Concurrent Requests, does not change when upgrading to Release 6.0 from an earlier release. This is deliberate and is intended to allow you to retain the pre-existing value even though Release 6.0 has a default value of 15 maximum concurrent requests. You can change this value on the Service Parameters Configuration window.

IP Phone Messenger (IPPM) User Does Not Have Callback Capability

An IPPM (IP Phone Messenger) user does not have callback capabilities if the user logs into IPPM on a phone where the user is not assigned to the line appearance. When a user logs in to the IPPM service on a Cisco Unified IP Phone and views the details of a MeetingPlace based meeting on the phone screen, the Callback and Join softkeys do not display when the user is not associated with a line appearance. Although the user has associated himself with a device on the Cisco Unified Communication Manager Administration End User Configuration window, the line appearance on the device itself must be configured with an association to the user in order for the softkeys to display on the phone.

Workaround:

Associate the line appearance to the end user by using Cisco Unified Communications Manager Administration.

Step 1 From Cisco Unified Communications Manager administration, choose **Device > Phone**.

The Find and List Phones window displays.

Step 2 Locate the phone and click the device name of that phone.

The Phone Configuration window displays.

Step 3 Locate the line and click it.

Step 4 Associate the line to the end user (near bottom of the window).

Note You will not have callback capabilities if you log in to a phone where you are assigned on the line appearance.

Monitoring Call Gets Dropped When Agent Call Is Put on Hold

When the agent IP phone uses SIP and the supervisor IP phone uses SCCP, the monitoring call gets set up correctly; however. when the agent call is put on hold, the supervisor gets disconnected and receives a fast busy tone.

To avoid this problem, you can change the signaling protocol on either the agent or supervisor, so both phones are using the same signaling protocol.

Note If you cannot apply that workaround, no way exists to prevent the disconnect; however, the supervisor can reinitiate a monitoring session from the CTI application, and a new monitoring call will be set up.

DVDROM Not Accessible After Upgrade

If you pull the DVD drive out or the DVD drive becomes not accessible during an upgrade, the grub.conf file may become corrupted.

If this happens, you may experience problems when you try to switch versions. For example, rebooting to the upgraded partition may fail, or the reboot may fail, or the reboot will result in a grub menu.

Workaround

You should open a TAC case.

Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration

In Cisco Unified Communications Manager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you delete a subsequent node in the Find and List Servers window, Cisco Unified Communications Manager Administration displays the following message: “You are about to permanently delete one or more servers. This action cannot be undone. Continue?”. If you click OK, the server gets deleted from the Cisco Unified Communications Manager database and is not available for use.

Tip When you attempt to delete a server from the Server Configuration window, a similar message as the one in the preceding paragraph displays. If you click OK, the server gets deleted from the Cisco Unified Communications Manager database and is not available for use.

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure:

Tip Before you perform the procedure, review the information in the “Deleting a Server” section on page 138, which provides important considerations on deleting a server.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, add the server, as described in the “Configuring a Server” section (Server Configuration chapter) in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform a 6.0(1) installation on it by using the 6.0(1) disk that Cisco provided in your software kit.

Tip Make sure that the version that you install on the subsequent node matches the version that runs on the first node (publisher) in the cluster.

If the first node in the cluster runs 6.0(1) and a service release (or engineering special), you must choose the **Upgrade During Install** option when the installation displays the installation options; before you choose this option, ensure that you can access the service release (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, refer to *Installing Cisco Unified Communications Manager 6.0(1).*

After you install Cisco Unified Communications Manager, configure the subsequent node, as described in the "Configuring a Subsequent Node" section in the document, *Installing Cisco Unified Communications Manager 6.0(1).*

Call History Might Get Lost When AAR Routes Over QSIG Trunk

When a call is forwarded to another cluster over a trunk/gateway by using QSIG because of insufficient bandwidth (Call Forward No Bandwidth - CFNB), call history might get lost.

If Phone A calls Phone B, which is in a low bandwidth location, with CFNR set to forward calls to Phone C, which is in a different cluster, and the QSIG protocol is used on the trunk/gateway, the original called party and the last redirecting party might not get passed to the destination party.

Extension Mobility Maximum Concurrent Requests Number Does Not Change After Upgrade

When you upgrade from Cisco Unified Communications Manager Release 4.x or 5.x to Cisco Unified Communications Manager Release 6,0(1), and you navigate to **System-->Service Parameters-->Cisco Extension Mobility,** you will see that the maximum concurrent requests value does not change after the upgrade. The value remains the same as it was for Cisco Unified Communications Manager Release 4.x or 5.x, even though the default value for the maximum concurrent requests for extension mobility in Cisco Unified Communications Manager Release 6.0(1x) is 15.

You can manually change this number to the system default of 15 or greater.

Upgrade Paths to Cisco Unified Communications Manager Release 6.0(1x)

You can upgrade directly to Cisco Unified Communications Manager Release 6.0(1) from these previous releases:

- 4.0(2a)
- 4.1(3)
- 4.2(3)
- 5.0(4)a
- 5.0(4)b
- 5.1(1)
- 5.1(2)

Cisco Unified Communications Manager Assistant Limitations with Cisco IP Communicator

Cisco IP Communicator does not support Cisco Unified Communications Manager Assistant Releases 5.1 and 6.0.

Translation Pattern Support

If a calling party transformation mask is configured for a translation pattern that is applied to a JTAPI application-controlled address, the application may see extra connections that are created and disconnected when both the calling and called party are observed. The system creates a connection for a transformed calling party instead of the actual calling party, and CiscoCall.getCurrentCallingParty() would return the transformed calling party, when only the called party is observed. In general, JTAPI might not be able to create the appropriate connection in the call, and might not be able to provide correct information for currentCalling, currentCalled, calling, called, and lastRedirecting parties.

For example, consider a translation pattern X that is configured with a calling party transformation mask Y and calledparty transformation mask B. If A calls X, the call goes to B. In this scenario

If the application is observing only B, JTAPI creates a connection for Y and B, and CiscoCall.getCurrentCallingParty() would return Address Y.

If the application is observing both A and B, a connection for A and B gets created, a connection for Y gets temporarily created and dropped, and CiscoCall.getCurrentCallingParty() would return Address Y.

Other inconsistencies could occur in the calling information if further features get performed on a basic call. Cisco recommends that you not configure a calling party transformation mask for a translation pattern that might get applied to JTAPI application-controlled addresses.

Subscribe Calendar 500 Internal Error

A large number of Cisco Unified Presence Communicator users (for example 150 or more), each with 30 or more contacts with calendar enabled, that log in within a short period of time can compromise the ability of the Microsoft Exchange server to process the requests. The Microsoft Exchange 2003 server will begin to return "500 Internal Server Error" response to most, if not all, requests. The Microsoft Exchange server may or may not recover from the load.

Note The exact conditions may vary from server to server; however, login rates of more than one per second may cause the condition. In some instances, this behavior can get triggered at a rate of one login per 30 seconds.

Maximum Trace Settings

The maximum recommended Cisco Unified Communications Manager trace settings is 2,500 files of 2 MB each, for SDI and SDL traces, for a combined total of 5000 files. You can increase SDI traces to 5,000 files if SDL traces are disabled, but not vice versa. All other components should stay within 126 MB bucket (for example, 63 files of 2 MB). If you increase logs past the recommended limit, system

performance gets reduced due to IOWAIT. After the system experiences IOWAIT related performance degradation, the only solution requires you to lower traces and use RTMT to remove all CCM/CTI SDI/SDL traces. For that reason, you should limit tracing to 5 GB for CCM and 5 GB for CTI.

Disabling the Advertise G.722 Codec Enterprise Parameter When You Are Using System Features

If you are experiencing feature interoperability issues, and you have the Cisco Unified Communications Manager enterprise parameter Advertise G.722 Codec set to Enabled, you should change the setting to Disabled (the default setting specifies Enabled) and update the device pools for the phones. When enabled, the enterprise parameter allows Cisco Unified IP Phones (such as 7971, 7970, 7941, 7961) to negotiate and use the G.722 codec when calls are within the same region.

If individual phone control and use of a specific codec type is required (for example, G.711), check the configuration of each phone (by using Phone Configuration) for the parameter Advertise G.722 Codec and change the setting to Disabled. Save and reset the device.

Note If the Advertise G.722 Codec enterprise parameter is set to Enabled, the administrator can override this setting by using the G722 Codec Enabled service parameter. This service parameter determines whether Cisco Unified Communications Manager supports G.722 negotiation for none, some, or all devices. Valid values specify Enabled for All Devices (support G.722 for all devices), Enabled for All Devices Except Recording-Enabled Devices (support G.722 for all devices except those that have call recording enabled), or Disabled (do not support G.722 codec).

For more information about the G.722 codec, see the "Using the G.722 Codec" section on page 126.

Using FTP to Upgrade to Cisco Unified Communications Manager Release 6.0(1x)

Even if enough disk space exists, if you upgrade to this release by using FTP, the upgrade might fail with an error message that states that not enough disk space exists to complete the upgrade.

If this happens, begin the upgrade again by using a different upgrade method (such as SFTP or LOCAL) or use different FTP server software.

Cisco Unified Personal Communicator LDAP Attribute Mappings

Be aware that Cisco Unified Personal Communicator LDAP attribute mappings are wrong for the Active Directory set of attribute mappings.

Before Cisco Unified Communications Manager Release 6.0(1), only one set of LDAP attribute mappings existed. In Cisco Unified Communications Manager Release 6.0(1), two sets of attribute mappings exist: for Netscape LDAP and for Active Directory LDAP. During an upgrade to this release, the default attribute mappings do not get correctly carried forward into the Cisco Unified Communications Manager Release 6.0(1) attribute mappings for Active Directory LDAP. (They correctly get carried forward for Netscape LDAP.)

This applies to default attribute mappings. Non-default attribute mappings (for example those explicitly specified by the user) properly get carried forward for both Netscape LDAP and Active Directory LDAP.

Before you upgrade to Cisco Unified Communications Manager Release 6.0(1x), make a note of the Cisco Unified Personal Communicator LDAP attribute mappings and enter the original values for the Active Directory set of attribute mappings

Terminal Server Causes RTMT to Display Repeating Syslog and Alert Messages

When a terminal server is connected to the serial port of a Cisco Unified Communications Manager server, the system generates a repeating alert message and corresponding syslog message similar to the following examples:

- Alert Message—SeverityMatch - Alert login(pam_unix)[12916]: check pass; user unknown
- Syslog Message—May 16 04:44:44 azo-cm-uc auth 5 mgetty[23127]: failed dev=ttyS0, pid=23127, login time out

This includes a router that is being used as a terminal server.

Cisco recommended that you configure **no exec** on the lines that are connected to the console of the other devices.

New and Changed Information in Cisco Unified Communications Manager 6.0(1a)

The following sections describe new features and changes that are pertinent to Cisco Unified Communications Manager, Release 6.0(1a) . The sections may include configuration tips for the administrator, information about users, and information about where to find more information

Basic Uninterruptible Power Supply (UPS) Integration

When Cisco Unified Communications Manager 6.0(1a) runs on an MCS 7825H2 or MCS 7835H2, basic integration to the following UPS models: 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 are supported. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, on MCS-7835H2, you can execute the “show ups status" CLI command to activate the feature (see “Command Line Interface Enhancements”).

On supported servers, the CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime and other relevant status information.

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

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

HP NC-Series Broadcom Firmware Updates Available for Supported NICs.

The upgrade includes

- iSCSI and UMP firmware upgrade support.
- An IPMI configuration command that allows IPMI to be enabled or disabled from the command line.

You can update firmware manually by downloading and booting from the HP Firmware Maintenance CD version 7.80 (10 May 07) that is located at
http://h18023.www1.hp.com/support/files/server/us/download/27225.html

Smart Array 6i Requires HD Firmware Update to Avoid POST Notification

You should upgrade hard drive models that experience excessive SCSI command timeout. Failure to upgrade may result in the bus down-shifting from Ultra 320 to Ultra 3.

Upgrade following hard disk models to the specified versions:

Table 2 Recommended Firmware Upgrades

Hard Disk Model	Upgrade to
BF018863B8, BF036863B9, BF072863BA	HPB6 B (4 Jan 07
BD146863B3, BD072863B2, BD036863AC, BD03697633	HPB8 B (4 Jan 07
BD14686225, BD07286224, BD03686223, BD07296B44, BD03695CC8	HPB6 E (4 Jan 07)
BD009635CB, BD00973623, BD018635CC, BD01873624, BD03663622, BD03673625, BC072638A2	BDCB D (4 Jan 07)
BD01865CC4, BD01875CC7, BD00965CC3, BD00975CC6, BD00415CBC, BD00425CC2	HPB6 D (4 Jan 07)
BD0096349A, BD009734A3, BD0186349B, BD018734A4	3B15 D (4 Jan 07)
BD00962A66, BD00972A69, BD01862A67, BD01872A6A	B008 D (4 Jan 07)

Table 2 Recommended Firmware Upgrades

Hard Disk Model	Upgrade to
BD00962373 BD00972374 BD01862376 BD01872377 and BC0367237A	BCJG D (4 Jan 07)
BD00912578 and BD01812579	BCJG D (18 Jan 07)
AD01836222, AD00935CCC, AD00435CCB	HPA6 C (16 Jan 07)
AD00933626 and AD01833627 drives version	ADCB D (4 Jan 07)
AD00932372 AD01832375 and AC03632378	ACJG D (4 Jan 07)

Workaround

You can update firmware manually by downloading and booting from the HP Firmware Maintenance CD version 7.80 (10 May 07) that is located at http://h18023.www1.hp.com/support/files/server/us/download/27225.html

CSCsj72914 Conference Calls Experience Poor Audio Quality

Conference calls using the software media resources (MTP, MOH, and CFB) on a CallManager 5.1(2) server experience poor audio quality when traversing a WAN with QoS implemented.

Since the RTP coming from Cisco Unified CallManager has a DSCP of 0x00 these packets can be queued and/or dropped behind other voice signaling and RTP packets at the WAN router. Depending on network conditions for the WAN link this can cause poor audio quality.

Current Condition

The release of Cisco Unified Communications Manager Release 6.0(1a) resolves this problem.

CSCsj61395 Spurious Error Message Displays During Installation of Locale COP Files on a Subscriber Server

Previously, when a user installed a locale COP file on a subscriber server, an error message displayed: “Status: Error Encountered”.

Current Condition

The release of Cisco Unified Communications Manager Release 6.0(1a) resolves this problem.

CSCsj55359 Installation Media Cannot Locate Available Patches

The installation media does not find the available upgrade patches.

Workaround

The release of Cisco Unified Communications Manager Release 6.0(1a) resolves this problem.

CSCsj42131 User with Incorrect Primary Extension in Directory Export

Caveat

After migration from Cisco Unified CallManager Release 4.x to Cisco Unified CallManager Release 5.x, the user gets associated with the wrong primary extension.

Current Condition

The release of Data Migration Assistant 6.0(1a) and Cisco Unified Communications Manager resolves this problem.

CSCsj22669 User and User Profile Association Issue In Directory Export

Caveat

Multiple CNN-profiles per user exist in the Cisco Unified CallManager Release 4.x directory. After an upgrade to Cisco Unified Communications Manager 6.0(1), despite a clean DMA run, lost/missing/incorrect login profiles and device associations exist.

Current Condition

The release of Data Migration Assistant 6.0(1a) and Cisco Unified Communications Manager resolves this problem.

CSCsi71128 DMA Requires a Long Time to Run

Caveat

When users upgrade to Cisco Unified Communications Manager Release 6.x, from releases prior to release 4.1(3), DMA execution takes a very long time in the pre-migration phase. If this occurs, the users should wait for completion. A delay in this phase of up to 23 hours for 45,000 devices has occurred.

Current Condition

The release of Data Migration Assistant 6.0(1a) and Cisco Unified Communications Manager resolves this problem.

CSCsi20684 CSS Call Forward All

Caveat

DMA fails to validate when invalid contents exist in the CSSForCFA table:

The need exists for DMA processing to handle invalid CSS failures more efficiently.

Current Condition

The release of Data Migration Assistant 6.0(1a) and Cisco Unified Communications Manager resolves this problem.

New and Changed Information in Cisco Unified Communications Manager 6.0(1)

The following sections describe new features and changes that are pertinent to Cisco Unified Communications Manager, Release 6.0(1) or later. The sections may include configuration tips for the administrator, information about users, and information about where to find more information.

Installation, Upgrade, Migration, and Disaster Recovery

The following sections describe the changes that were made to the installation, upgrade, and disaster recovery procedures in Cisco Unified Communications Manager 6.0(1):

Installation Overview

- In addition to installing Cisco Unified Communications Manager, the installation program supports installing Cisco Unity and Cisco Unified Communications Manager Business Edition.
- Now you can specify the Application User account name during installation.
- You can generate preexisting configuration information that is required for an installation by using an online Answer File Generator (http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-utilpage). You can use the resulting answer file rather than entering the configuration information manually during the installation procedure.

Software Upgrades

You can initiate and manage upgrades by using the **utils system upgrade** CLI command.

Disaster Recovery System

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Where to Find More Information

- *Disaster Recovery System Administration Guide*
- *Data Migration Assistant User Guide*
- *Upgrading Cisco Unified Communications Manager Release 6.0(1)*
- *Installing Cisco Unified Communications Manager Release 6.0(1)*
- *Cisco Unified Communications Operating System Administration Guide, Release 6.0(1)*

Cisco Unified Communications Operating System Administration

For Cisco Unified Communications Manager 6.0(1), you can perform many common system administration functions through the Cisco Unified Communications Operating System.

This chapter comprises the following topics:

Overview

You cannot log in to Cisco Unified Communications Operating System and Cisco Unified Communications Manager Administration at the same time.

Browser Requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Communications Operating System Administration by using the following h:

- Microsoft Internet Explorer version 6.x
- Netscape Navigator version 7.1

Note Cisco does not support or test other browsers, such as Mozilla Firefox.

Platform Status and Configuration Enhancements

This release removed the **Logs** item from the **Show** menu.

Settings Enhancements

This release added the **Version** item to the **Settings** menu.

Restart Options Enhancements

The system restart and version switching features moved from a **System Restart** menu to the **Settings** > **Version** window.

Security Configuration Enhancements

The reorganized security features and the Security menu moved all certificate management features to the **Security** > **Certificate Management** window. All IPSec management features moved to the **Security** > **IPSec Management** window.

Software Upgrades Enhancements

- You can initiate and manage upgrades by using the **utils system upgrade** CLI command.
- The upgrade file that you use to upgrade from a 6.x release to a later 6.x release now exists as an ISO image file. Previously the upgrade file had a different file format.
- You can delete files from the TFTP server.

Command Line Interface Enhancements

This release adds the following CLI commands:

- **utils system upgrade**—Allows you to initiate and manage upgrade server upgrades.
- **show tech dbstateinfo**—Shows the state of the database.
- **show tech dbintegrity**—Shows the integrity of the database.
- **show tech prefs**—Displays database settings.
- **utils fior**—Monitors I/O on the server.
- **show ups**—Shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started
- **show environment**—Displays information about the server hardware
- **show memory**—Displays information about the server memory

Where to Find More Information

- *Cisco Unified Communications Operating System Administration Guide*

Cisco Unified Communications Manager Administration

The following sections describe the Cisco Unified Communications Manager Administration enhancements:

System Architecture Changes

Cisco Unified Communications Manager Administration Release 6.0 introduces the following changes to the way the database behaves during installation or upgrade:

- Enhancements to the database CLI command, **show tech dbstateinfo**, show active SQL statements and which process is executing them.
- The database no longer uses “CCMAdministrator” as a default super userid for administration during installation. Instead, the installation process asks for the user ID of the administrator. You should use this new userid when you are logging in to Cisco Unified Communications Manager Administration for the first time on fresh installations.
- Information from the installation framework to fit the topology that is being installed provides basis for the Cisco Unified Communications Manager database that is now conditionally sized. It provides four different sizes:
  - Super cluster
  - Normal (30K phones)
  - Cisco Unified Communications Manager Business Edition (500 phones)
  - Serviceability support (100 phones)—For standalone Unity Connection

- When a software upgrade from Cisco Unified Communications Operating System Administration from 5.x and beyond is performed, changes that are made during the upgrade for user-facing features will no longer get lost. This includes updates for the following features:
  - Call Forward All (CFA)
  - Message Waiting Indicator (MWI)
  - Privacy Enable/Disable
  - Do Not Disturb (DND) Enable/Disable
  - Extension Mobility (EM) Login
  - Log Out of Hunt Group
  - Device Mobility
  - CTI CAPF status for end users and application users
  - Credential hacking and authentication

Note Upgrades from 4.x to 6.x require that the user log out and then log back in.

- Replication alarms and perfmon counters have meaning on subscribers servers as well as the publisher server.
- Loss of connectivity to the publisher server will not prohibit the setting of call-processing user facing features such as call forward and message waiting indicator. This means that you can forward your phone or log in by using extension mobility even when the publisher server is not accessible.

Change notification will queue up as replication queues up and proceed as replication proceeds. This should alleviate previous anomalous behavior on subscriber servers that have experienced a time where the publisher server was not available, and services on the subscriber servers did not receive one or more change notification events from the publisher server.

General Administration Enhancements

Cisco Unified Communications Manager Administration Release 6.0 supports JSPs, STRUTS framework, and Java. The following requirements apply to Cisco Unified Communications Manager Administration:

- Microsoft Internet Explorer (IE) 6.0
- Netscape 7.1

Note This release does not support Microsoft IE 5.5 and Netscape 7.0.

Navigating to IP Telephony Applications Within Cisco Unified Communications Manager Enhancements

After you log on, the main Cisco Unified Communications Manager Administration window redisplays. The window includes the drop-down list box in the upper, right corner called **Navigation**. To access the applications in the drop-down list box, choose the program that you want and click **Go**. The choices in the drop-down list box include the following Cisco Unified Communications Manager applications:

- Cisco Unified Communications Manager Administration—Shows the default when you access Cisco Unified Communications Manager. Use Cisco Unified Communications Manager Administration to configure system parameters, route plans, devices, and much more.
- Cisco Unified Serviceability—Takes you to the main Cisco Unified Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.
- Cisco Unified OS Administration—Takes you to main Cisco Unified OS Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log off from any other application before you can log in to this application.
- Cisco Unity Connection Administration—Takes you to the main Cisco Unity Connection Administration window to configure voice messaging, integrated messaging, speech recognition capabilities, and call-routing rules. This menu option applies only to Cisco Unified Communications Manager Business Edition systems.
- Cisco Unity Connection Serviceability—Takes you to the main Cisco Unity Connection Serviceability window to configure trace files and alarms and to activate and deactivate services for Cisco Unity Connection. This menu option applies only to Cisco Unified Communications Manager Business Edition systems.
- Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. You must log off from any other application before you can log in to this application.

After you log in to Cisco Unified Communications Manager Administration, you can access all applications that display in the Navigation drop-down list box, except for the Cisco Unified Communications Operating System Administration and Disaster Recovery System, without having to log in to each application. You cannot access the Cisco Unified Communications Operating System Administration or Disaster Recovery System GUIs with the same username and password that you use to access Cisco Unified Communications Manager Administration. To access these applications from Cisco Unified Communications Manager Administration, you must first click the **Logout** button in the upper, right corner of the Cisco Unified Communications Manager Administration window; then choose the application from the Navigation drop-down list box and click **Go**.

If you have already logged in to one of the applications that display in the Navigation drop-down list box (other than Cisco Unified Communications Operating System Administration or Disaster Recovery System), you can access Cisco Unified Communications Manager Administration without logging in. From the Navigation drop-down list box, choose Cisco Unified Communications Manager Administration and click **Go**.

Where to Find More Information

- Introduction, *Cisco Unified CallManager Administration Guide*

Localizing Cisco Unified Communications Manager Administration

Cisco Unified Communications Manager Release 6.0 incorporates the following localization capabilities:

- End User Configuration windows get localized. Other configuration windows that share the End User Configuration get localized.
- To see the localization, set the browser to the language that is required. If that language locale is loaded, the configuration windows will display as localized.

Migration Tips

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager supports up to 3500 managers and 3500 assistants for a total of 7000 users. To support 7000 users, the administrator must configure multiple active Cisco IP Manager Assistant servers by enabling and setting service parameters. Administrators can configure up to three active Cisco IP Manager Assistant servers, each managing up to 2500 managers and assistants. Each server can also have a backup server. Configure the Cisco IP Manager Assistant servers by using the Advanced Service Parameters, Enable Multiple Active Mode, Pool 2: Cisco IPMA Server, and Pool3: Cisco IPMA Server. If you are migrating from a release previous to Cisco Unified Communications Manager Release 6.0(1), all managers and assistants will get migrated to Pool 1 (the default).

Check Box to User Group

The following check boxes in Cisco Unified Communications Manager Administration get migrated to user groups when you upgrade from Release 4.2 to Release 6.0.

Check Box Name in Releases Before 5.0	Functionality Migrated to This User Group
Enable Computer Telephony Integration (CTI) Application Use	Standard CTI Enabled
Enable CTI Super Provider	Standard CTI Allow Control of All Devices
Enable Calling Party Number Modification	Standard CTI Allow Calling Number Modification
Call Park Retrieval Allowed	Standard CTI Allow Call Park Monitoring

General Changes That Were Made to Multiple Windows

You can find the following changes on multiple Cisco Unified Communications Manager Administration windows:

- Clear Filter and + and - buttons—Found on the Find/List windows. To add additional search criteria click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the **Clear Filter** button to remove all added search criteria.
- Device Pool—Used by many configuration windows for certain configuration details (for example, date/time group). Release 6.0 removed some fields from the device pool and added them to the common device configuration, so some configuration windows will need to include information about device pools and common device configurations for certain configuration details (for example, softkey templates).
- Common Device Configuration—A new configuration window that provides information about softkey templates, MOH, and MLPP. This common device configuration gets assigned to phones in the Phone Configuration window.

Service Parameter Changes

Cisco Unified Communications Manager 6.0 supports the following service parameter changes:

- Advance Ad Hoc Conference Enabled (introduced in release 4.2(3))
- Nonlinear Ad Hoc Conference Linking Enabled (introduced in release 4.2(3))

- Always Display Original Dialed Number (introduced in release 4.2(3))
- Call Diagnostics Enabled (introduced in release 4.2(1))
- Hold Reversion Duration timer (introduced in release 4.2(3))
- Hold Reversion Notification Interval (introduced in release 4.2(3))
- Overlap Receiving Flag for H.323 (introduced in release 4.2(1))
- Hunt Group Logoff Notification (introduced in release 4.2(1))
- Enforce Privacy Setting on Held Calls (introduced in release 4.2(1))
- Bundle Outbound SCCP Messages timer (introduced in release 4.2(3))
- Play Recording Notification Tone To Observed Target (introduced in release 6.0(1))
- Play Recording Notification Tone To Observed Connected Parties (introduced in release 6.0(1))
- Play Monitoring Notification Tone To Observed Target (introduced in release 6.0(1)
- Play Monitoring Notification Tone To Observed Connected Parties (introduced in release 6.0(1))
- Enable/Disable Multiple Active Mode
- Pool 2: Cisco IPMA Server (Primary) IP Address
- Pool 2: Cisco IPMA Server (Backup) IP Address
- Pool 3: Cisco IPMA Server (Primary) IP Address
- Pool 3: Cisco IPMA Server (Backup) IP Address
- CUP PUBLISH Trunk
- Default PUBLISH Expiration Timer
- Minimum PUBLISH Expiration Timer
- Retry Count for SIP Publish
- SIP Publish Timer
- BLF Status Depicts DND
- G722 Codec Enabled
- iLBC Codec Enabled
- Built-in Bridge Enable
- Maximum Concurrent Requests now an advanced service parameter
- Delay before ringing cell phone timer
- Answer too late timer (also known as Maximum cell phone ring timer)
- Answer too soon timer (also known as Minimum cell phone ring timer)
- CFA CSS Activation Policy
- Maximum Number of Threads and Process
- SIP Station UDP Port Throttle Threshold
- SIP Trunk UDP Port Throttle Threshold

Enterprise Parameter Changes

Cisco Unified Communications Manager 6.0 supports the following enterprise parameter changes:

- Phone Personalization

- Enable Caching

Locations and Region Enhancements

Cisco Unified Communications Manager supports up to 1000 locations and up to 2000 regions. The following limitations and restrictions apply:

- Configure as many regions as possible to Use System Default for inter/intra region audio codecs and video bandwidth.
- Configure as many locations as possible to Use System Default for the RSVP policy.

This enhancement requires an MCS 7845H1 or higher server.

System Menu Changes

The following changes occurred in the System menu:

- Device Pool—Field changes
- Device Mobility (New)—Submenus
  - Device Mobility Group
  - Device Mobility Info
- Physical Location (New)
- Application server—New fields

Call Routing Menu Changes

The following changes occurred in the Call Routing menu:

- Intercom (New)
  - Intercom Route Partition
  - Intercom Calling Search Space
  - Intercom Directory Number
  - Intercom Translation Pattern
- Directed Call Park (new)
- Directory Number
  - New Calling Search Space Activation Policy field
- Meet-Me Number/Pattern
  - Minimum Security Level (new field)
- Transformation Pattern (new)
- Mobility Configuration (new)

Media Resources Menu

The following changes occurred in the Media Resources menu:

- Mobile Voice Access (new)

- Conference Bridge
  - Common Device Configuration (new field)
  - Cisco IOS Enhanced Conference Bridge contains new field: Device Security Mode, which supports encrypted and nonsecure bridges.

Voice Mail Menu

No changes occurred to the Voice Mail menu.

Device Menu Changes

The following changes occurred in the Device menu:

- Phone
  - New device types 7921, 7931, and 3951 (not available to North American and European markets)
  - Common Device Configuration (new)
  - Device Mobility Mode (new)
  - Phone Personalization (new)
  - Primary Phone (new)
  - Logged Into Hunt Group (new)
  - Remote Device (new)
  - Do Not Disturb (new)
  - Mobility User ID (Dual-mode phones only) (new)
  - Outbound Call Rollover (new)
  - Actively Logged in Device Report (new)—Access this window from the Related Links drop-down list box on the Find and List Phones window.
  - Association Information Line configuration— Two new fields on the Directory Number Configuration window: Recording Option and Recording Profile
- Remote Destination (new)
- Device > Device Settings
  - Common Device Configuration (new)
  - Access List (new)
  - Common Phone Profile (updated)—DND and Phone Personalization
  - Remote Destination Profile (new)
  - Recording Profile (new)

Application Menu Changes

No changes.

User Management Menu

The following changes occurred in the User Management menu:

- Credential Policy Default (new)
- Credential Policy (new)
- Application User
  - Edit Credential (new field)
- End User Configuration
  - Edit Credential (new field)

Bulk Administration Menu

Bulk Administration contains the following new menu items in release 6.0:

- Phones > Add/Update Intercom (new)
- Users
  - Line Appearance (new)
  - Reset Password/PIN (new). Contains two menus for Query and Custom File.
- Gateways > Insert Gateways (now supports VG224)
- Gateways > Gateway File Format (new)
- Mobility (new)
  - Access List (new)
  - Remote Destination (new)
  - Remote Destination Profile (new)
- Config Tool (new)

For more information about the Bulk Administration application, see Cisco Unified Communications Manager Bulk Administration Features, page 70.

Where to Find More Information

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

Cisco Unified Communications Manager Features

The following sections describe the Cisco Unified Communications Manager 6.0 feature enhancements:

AAC/iLBC Voice Codec Support

Release 5.1(1) of Cisco Unified Communications Manager added support for the Advanced Audio Codec (AAC) and the Internet Low Bit Rate Codec (iLBC), but without any changes to the user interface. Release 6.0(1) of Cisco Unified CallManager Administration added the AAC and iLBC audio codecs to the user interface.

The Advanced Audio Codec (AAC) specifies a wideband voice codec that provides improved voice fidelity. This codec also provides equal or improved sound quality over older codecs with lower bit rates.The SIP call protocol supports use of the AAC as an audio codec. Use the AAC audio codec for calls between SIP phones.

The Internet Low Bit Rate Codec (iLBC) enables graceful speech quality degradation in a lossy network where frames get lost. Be aware that the iLBC is suitable for real-time communications, such as telephony and video conferencing, streaming audio, archival, and messaging.The iLBC has good error resilience character in a lossy network. When a link in the network has a high error rate, the administrator can configure the region pair as lossy, which in turn enables selection of iLBC for that link if iLBC is configured.The SIP, SCCP, and MGCP call protocols support use of the iLBC as an audio codec.

When you assign the SIP trunk or third-party SIP phone with the MTP Required option enabled to the device pool for that region, you must verify that the region relationship between the SIP device and the MTP device is configured to use a codec with equal or greater bandwidth (G.711 or Wideband/AAC codec). See the "SIP Third-Party Phones Enhancements" section on page 53 and the "SIP Trunk Enhancements" section on page 54 for more information.

Cisco Unified Communications Manager Administration Configuration Tips

The following configuration tips apply to the AAC and iLBC audio codecs:

- To specify the AAC audio codec, configure the Wideband/AAC codec in the Region Configuration window of Cisco Unified Communications Manager Administration.
- To specify the iLBC audio codec, configure the G.728/iLBC codec in the Region Configuration window of Cisco Unified Communications Manager Administration.

GUI Changes

In Release 6.0(1) of Cisco Unified Communications Manager Administration, the Region Configuration window adds the AAC and iLBC audio codecs to the list of audio codecs that can be configured. In Release 5.1(1), the administrator needed to choose the G.728 codec (for iLBC) and Wideband codec (for AAC).

Where to Find More Information

- System-Level Configuration Settings, *Cisco Unified Communications Manager System Guide*
- Understanding Session Initiation Protocol (SIP), *Cisco Unified Communications Manager System Guide*
- Region Configuration, *Cisco Unified Communications Manager Administration Guide*

Advanced Ad Hoc Conference

Cisco Unified Communications Manager Release 4.2(3) made enhancements to the ad hoc conference feature and provided the following advanced capabilities in release 6.0:

- A conference participant other than the controller can now add or remove participants.
- Conference participants can now chain multiple ad hoc conferences together in linear or nonlinear fashion.
- You can enable or disable these advanced capabilities by setting the value of two new service parameters (see Service Parameter Changes, page 22).

When multiple conferences are chained together, all the participants can hear and talk to each other; however, the ConfList softkey does not display a full list of all the participants in all the chained conferences. ConfList can only display the participants in its own conference and displays a linked conference as "Conference." The conferences do not get merged into a single conference.

Where to Find More Information

- *Cisco Unified Communications Manager Administration Guide*

- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Cisco Unified IP Phone User Guides*
- Release Notes for Cisco Unified Communications Manager Release 4.2(3)

Audible Message Waiting Indicator

Audible MWI, an accessibility feature, notifies visually impaired users of voice messages. When a voice message occurs on a line and the user goes off hook on that line, the phone plays a stutter dial tone to indicate the presence of voice message.

For non-visually impaired users, audible MWI provides a redundant indication of voice messages.

Cisco Unified Communications Manager Administration Configuration Tips

Use Directory Number Configuration to set the Audible Message Waiting Indicator Policy. This field configures an audible message waiting indicator policy for a line on the phone.

GUI Changes

New Audible Message Waiting Indicator Policy field displays on the Directory Number Configuration window. This field offers the following configurable settings:

- Off
- On—When this option is chosen, you will receive a stutter dial tone when you take the handset off hook.
- Default—When this option is chosen, the phone uses the default that was set from the Audible Message Waiting Indicator Policy clusterwide service parameter. This service parameter offers the following settings:
  - Off
  - On

BAT Considerations

The Line Template Configuration window in BAT contains the Audible Message Waiting Indicator Policy field.

Where to Find More Information

- Directory Number Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone, *Cisco Unified Communications Manager System Guide*

Barge Enhancements

Nonsecure or authenticated Cisco Unified IP Phones that are running firmware release 8.3 or later can now barge encrypted calls.The security icon indicates the security status for the conference. (See the "Secure Conference Icon" section on page 74.)

- Due to bandwidth requirements, Cisco Unified IP Phones 7940 and 7960 do not support barge from an encrypted device on an active encrypted call. The barge attempt will fail. A tone plays on the initiator phone to indicate that the barge failed.

- Encrypted Cisco Unified IP Phones that are running firmware release 8.2 or earlier can only barge an active call as authenticated or nonsecure participants.
- If a caller barges a secure SCCP call, the system uses an internal tone-playing mechanism at the target device, and the status remains secure.
- If a caller barges a secure SIP call, the system provides tone-on-hold, and Cisco Unified Communications Manager classifies the call as nonsecure during the tone.

Cisco Unified Communications Manager Administration Configuration Tips

To secure conferences with barge, configure phones to use encrypted mode.

Where to Find More Information

- Barge and Privacy Release, *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Troubleshooting Guide*

Call Diagnostics and Voice Quality Metrics

Cisco Unified Communications Manager Release 4.2(1) allowed you to configure Cisco Unified IP Phones to collect call diagnostics and voice quality metrics by setting the Call Diagnostics Enabled service parameter to True in Cisco Unified Communications Manager Administration. You can access the metrics to monitor voice quality and troubleshoot network problems. T*he Call Statistics screen on the phone displays counters, statistics, and voice quality metrics in the following ways:*

- *During call—You can view the call information by pressing the ? button twice rapidly.*
- *After the call—You can view the call information that was captured during the last call by displaying the Call Statistics screen*

Note *You can remotely view the call statistics information by using a web browser to access the Streaming Statistics window.*

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use statistical metrics that are based on concealment events.

To use the metrics for monitoring voice quality, record the typical scores under normal conditions of zero packet loss and use the metrics as a baseline for comparison.

Where to Find More Information

- Troubleshooting Cisco Unified IP Phones, *Cisco Unified IP Phone Administration Guides*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Release Notes for Cisco Unified Communications Manager Release 4.2(1)

Call Forward Enhancements

Cisco Unified Communications Manager Release 4.2(1) made the following enhancements to the forwarding and Automated Alternate Routing (AAR) logic to redirect calls that cannot be connected due to no bandwidth or an unregistered directory number:

- No Bandwidth

This enhancement applies AAR treatment to calls that are blocked due to insufficient bandwidth by using the AAR Settings fields (AAR Destination Mask, AAR Voicemail Enabled).

- Unregistered Phone

  This enhancement forwards calls that are routed to a directory number with no registered devices.

Where to Find More Information

- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(1)*

Call Forward All Calling Search Space Backward Compatibility

This enhancement allows Cisco Unified Communications Manager Release 4.x customers who are using device mobility and extension mobility to upgrade to Cisco Unified Communications Manager Release 6.0 without loss of functionality.

In the Directory Number Configuration window, in the Call Forward and Call Pickup Setting section, a new option specifies Calling Search Space Activation Policy.

Three possible values exist for this option:

- Use System Default
- With Configured CSS
- With Activating Device/Line CSS

If you select the With Configured CSS option, the Forward All Calling Search Space that is explicitly configured in the Directory Number Configuration window controls the forward all activation and call forwarding. If the Forward All Calling Search Space is set to None, no CSS gets configured for Forward All. A forward all activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and Secondary Calling Search Space for Forward All occurs during the forward all activation.

If you prefer to utilize the combination of the Directory Number Calling Search Space and Device Calling Search Space without explicitly configuring a Forward All Calling Search Space, select With Activating Device/Line CSS for the Calling Search Space Activation Policy. With this option, when Forward All is activated from the phone, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All automatically get populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device.

With this configuration (Calling Search Space Activation Policy set to With Activating Device/Line), if the Forward All Calling Search Space is set to None, when forward all is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space gets used to verify the forward all attempt.

If you configure the Calling Search Space Activation Policy to Use System Default, the CFA CSS Activation Policy clusterwide service parameter determines which Forward All Calling Search space will be used. If the CFA CSS Activation Policy service parameter gets set to With Configured CSS, Forward All Calling Search Space and Secondary Calling Search Space for Forward All will get used for Call Forwarding. If CFA CSS Activation Policy service parameter gets set to With Activating Device/Line CSS, Forward All Calling Search Space and Secondary Calling Search Space for Forward All automatically will get populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device.

CFA CSS Activation Policy Service Parameter

The new service parameter (CFA CSS Activation Policy) supports this enhancement. In the Service Parameter Configuration window, this parameter displays in the Clusterwide Parameters (Feature - Forward) section:

- With Configured CSS (default)
- With Activating Device/Line CSS

When the Calling Search Space Activation Policy is set to Use System Default, the value of the CFA CSS Activation Policy service parameter determines the Call Forward All CSS.

When the option With Configured CSS is selected, the primary and secondary CFA Calling Search Space get used. When the option With Activating Device/Line CSS is selected, the primary and secondary CFA Calling Search Space get updated with primary line Calling Search Space and activating Device Calling Search Space.

By default, the system sets the value of the CFA CSS Activation Policy service parameter to With Configured CSS.

Roaming

When a device is roaming in the same device mobility group, Cisco Unified Communications Manager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the system sets CFA CSS to None, and the CFA CSS Activation Policy gets set to With Activating Device/Line CSS, then:

- The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.
- If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS get used as the CFA CSS.
- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.

For more information about configuration options for Call Forward All, see the Directory Number Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*, and the Understanding Directory Numbers chapter in the *Cisco Unified Communications Manager System Guide*.

Call Forward Overriding

Configure the behavior of this Cisco Unified Communications Manager feature, which was introduced in release 4.2(3), by using the service parameter, CFA Destination Override. When the feature is enabled on Cisco Unified Communications Manager, it allows the CFA Target to reach the CFA Initiator for important calls. TSP applications that monitor the CFA initiator will receive calls as normal if the call is initiated from the CFA target.

No TSP interface change exists for this Cisco Unified Communications Manager feature.

Where to Find More Information

- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(3*)

Call Pickup Notification

This feature allows users to receive an audio and/or visual alert when a call rings on a phone in pickup groups in which they are a member. For multiple line phones, the alert applies for pickup groups that are associated with the primary line only.

You can configure the following notification parameters in the Call Pickup Group Configuration window:

- Type of notification (audio, visual, both, or neither)
- Content of the visual notification message (called party identification, calling party identification, both, or neither)
- Number of seconds delay between the time the call comes into the original called party and the notification to the rest of the call pickup group members

You can configure the type of call pickup group audio notification that is provided for a line when a phone is idle or active by choosing the line in the Phone Configuration window.

Where to Find More Information

- Call Pickup Group, *Cisco Unified Communications Manager Features and Services Guide*
- Directory Number Configuration Settings, *Cisco Unified Communications Manager Administration*
- Advanced Call Handling, phone user guides

Cisco Messaging Interface Enhancements

The Cisco Messaging Interface (CMI) allows you to connect a simplified message desk interface (SMDI)-compliant external voice-messaging system with the Cisco Unified Communications Manager. The CMI service provides the communication between a voice-messaging system and Cisco Unified Communications Manager. The SMDI defines a way for a phone system to provide a voice-messaging system with the information that is needed to intelligently process incoming calls.

Introduced in Cisco Unified Communications Manager Release 4.2(1), you can now configure the CMI service parameters to define an alternate directory number and partition to be used when a non voice mail pilot number is dialed.

Note Users who have additional applications that are running on the voice-messaging system that require SMDI can configure the additional directory number (alternate DN). CMI will intercept all calls to this DN and generate an SMDI message over the serial cable to the server that is running the additional application. You make the partition for the alternate DN relevant online if you specify the alternate DN.

Where to Find More Information

- SMDI Voice Mail Integration, *Cisco Unified Communications Manager System Guide*

Cisco Unified Communications Manager T1 CAS Hookflash Transfer Support

Hookflash transfer defines a signaling procedure that allows a device, such as a voice-messaging system, to transfer a call to another destination. While the device is connected to Cisco Unified Communications Manager through a T1 CAS gateway, the device performs a hookflash procedure to perform the call transfer. Cisco Unified Communications Manager responds to the hookflash procedure by using a blind transfer to move the call. When the call transfer completes, the voice channel that connected the original call to the device gets released.

Cisco Unified Communications Manager Release 4.2(1) introduced the hookflash transfer on the T1 CAS ports of all Media Gateway Control Protocol (MGCP) gateways (both IOS and non-IOS gateways).

Where to Find More Information

- Understanding Cisco Unified Communications Manager Voice Gateways, *Cisco Unified Communications Manager System Guide*. (This chapter contains a summary of gateway model information. Every model that lists the T1 CAS port type supports hookflash transfer on those ports.)

Cisco Unified Phone Application Suite

Cisco Unified Phone Application Suite offers a series of application suites that run on Cisco Unified IP Phones. Cisco Unified Phone Application Suite provides unified access to Cisco and third-party services and applications and supports a common look and feel.

Cisco Unified Phone Application Suite supports the following features:

- Desktop (PC) GUI Application
- Support for personalized ringtone on the IP phone, with graphical sound editor
- Support for personalized wallpaper on the IP phone, with graphical image editor
- Click-to-dial from Microsoft Office products; outgoing-call history from the desktop application and re-dial from outgoing-call history
- Cisco Unified Phone View component of Cisco Unified Phone Application Suite allows voicemail and meeting management on phone screen with:
  - Cisco Unity and Cisco Unity Connection
  - Cisco Unified MeetingPlace Express

Cisco Unified Communications Manager Administration Configuration Tips

- To configure the Cisco Unified Phone Application Suite desktop application for phones, the administrator must set the Phone Personalization enterprise parameter to Enabled (disabled by default). In addition, the following configuration windows contain the Phone Personalization field: Phone Configuration and Common Phone Profile.

Enterprise Parameter Changes

- Phone Personalization

GUI Changes

- Phone Configuration—Choose **Device > Phone** and click **Find** or **Add New**. Phone Personalization displays as a field on the Phone Configuration window.
- Common Phone Profile—Choose **Device > Device Settings > Common Phone Profile** and click **Find** or **Add New**. Phone Personalization displays as a field on the Phone Configuration window.

User Tips

Cisco Unified Phone Application Suite supports the following Cisco Unified IP Phones:

- 7906G, 7911G, 7961G, 7961G-GE, 7941G, 7941G-GE, 7970G, 7971G

Where to Find More Information

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

- Common Phone Profile Configuration, *Cisco Unified Communications Manager Administration Guide*
- Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Phone Application Suite Installation and User Guide*

Connected Number Display

When a call routes through a translation or route pattern, routes to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application, the connected number display updates to show the modified number or redirected number.

The Connected Number Display restriction restricts the connected line ID presentation to dialed digits only for the duration of the call.

Where to Find More Information

- Call Display Restrictions, *Cisco Unified Communications Manager Features and Services Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(3)*

Credential Policy and User Authentication

Cisco Unified Communications Manager authenticates user login credentials before allowing system access. To help secure user accounts, administrators can now specify settings for failed logon attempts, lockout durations, password expirations, and password requirements in Cisco Unified Communications Manager Administration. These authentication rules form a credential policy.

Credential policies apply to application users and end users. At installation, Cisco Unified Communications Manager assigns the system Default Credential Policy to end user passwords, end user PINS, and application user passwords.

Cisco Unified Communications Manager does not provide default credentials. At installation, the system applies the application password that you configured at installation to all application users.

- Upgrades from 5.x releases automatically migrate end user passwords and PINs.
- Upgrades from 4.x releases assign a default password and PIN to end users during installation

If you enable the trivial credential checks setting in the applied policy, the system disallows credentials that are easily hacked.

You can assign new credential policies and new credentials after installation for account groups or individual users. When you add a new user to the Cisco Unified Communications Manager database, the system assigns the default policy. You can change the assigned policy, user credentials, and manage user authentication events in Cisco Unified Communications Manager Administration.

Credential policies do not apply to OS users or CLI users. These administrators use standard password verification procedures that the OS supports.

Credential policy settings in Cisco Unified Communications Manager Administration do not apply if your system uses LDAP authentication.

The authentication function in Cisco Unified Communications Manager authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encodes/decodes or encrypts/decrypts user credentials for data storage.

Because Cisco Unified Communications Manager Java Telephony Applications Programming Interface (JTAPI) and Telephony Applications Programming Interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that react to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Cisco Unified Communications Manager Administration Tips

The credential policy settings define the parameters that Cisco Unified Communications Manager uses during the authentication process:

- You define credential policies with the Credential Policy window (**User Management > Credential Policy**).
- You assign policies to groups in the Credential Policy Default window (**User management > Credential Policy Default**).
- You can change or view credential information for application and end users in the Credential Configuration window, which you access with the Edit Credential button in the user configuration window (**User Management > End User** and **User Management > Application User**).

Enterprise Parameter Changes

- To improve performance, administrators can configure the enterprise parameter “Enable Caching” to True. This eliminates the need for Cisco Unified Communications Manager to perform a database lookup or invoke a stored procedure for every single login request, thereby increasing system efficiency. An associated credential policy does not get enforced until the caching duration expires.

  This setting applies to all Java applications that invoke user authentication. The system ignores this setting for LDAP authentication.

Where to Find More Information

- Credential Policy, *Cisco Unified Communications Manager System Guide*
- Application User Configuration, *Cisco Unified Communications Manager Administration Guide*
- Credential Policy Default Configuration, *Cisco Unified Communications Manager Administration Guide*
- Credential Policy Configuration, *Cisco Unified Communications Manager Administration Guide*
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*

CTI Enhancements

CTI enhancements support new functionality in release 6.0:

- New Standard CTI user groups for monitor and record
- Expanded SIP support (see the “SIP Endpoints Support” section on page 50). Line-side SIP includes CTI functionality, which allows CTI applications such as Cisco Unified Communications Manager Assistant to support SIP on Cisco Unified IP Phones (for example, Cisco Unified IP Phone 7961). Be aware that CTI capabilities on phones that are using SIP are equivalent to those on phones that are using SCCP with a few exceptions. Some CTI features that are supported on phones that are using SIP include display text, set lamp, play tone, call park, and privacy support.
- Support for mobility and device mobility

Cisco Unified Communications Manager Administration Configuration Tips

- If a CTI application monitors calls, you must add the application to the Standard CTI Allow Call Monitoring user group. If the CTI application records calls, you must add the application to the Standard CTI Allow Call Recording user group.
- If a user will be call monitoring or call recording, you must add the end user to the Standard CTI Allow Call Monitoring and Standard CTI Allow Call Recording user groups.
- If using CTI ports with mobility or device mobility, configure the appropriate fields on the CTI Port Configuration window.

GUI Changes

- Standard CTI Allow Call Monitoring—This user group allows an application to monitor calls. Choose **User Management > User Group** and click **Find**.
- Standard CTI Allow Call Recording—This user group allows an application to record calls. Choose **User Management > User Group** and click **Find**.
- CTI Port—The CTI Port Configuration window includes new fields, check boxes, and Related Links:
  - Common Device Configuration
  - Device Mobility Mode
  - Logged Into Hunt Group
  - Remote Device
  - Add a New Line Appearance
  - Copy to Remote Destination Profile
  - Add a new intercom

Where to Find More Information

- Computer Telephony Integration, *Cisco Unified Communications Manager System Guide*
- Understanding Session Initiation Protocol, *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager JTAPI Developer Guide*
- *Cisco Unified Communications Manager TAPI Developer Guide*

Device Mobility

Cisco Unified Communications Manager uses IP subnets and device pools that contain location information to determine a device home location. By linking IP subnets to locations, the system can determine whether a device is at its home location or a remote location and register the device accordingly.

To support device mobility, modifications to the device pool structure separate the user information from the location and mobility information. Introduced in Cisco Unified Communications Manager Release 4.2(1), the device pool now contains the information that pertains to the device itself and to device mobility. An added common device profile allows you to configure all the user-related information. You must associate each device with the common device profile for user-based information.

Note Device pools that were already configured automatically migrate to the new structure as part of the upgrade to Cisco Unified Communications Manager Release 6.0(1).

In addition to the device pool and common device profile, device mobility uses device mobility groups, physical locations, and device mobility information to determine device identity and roaming properties and configuration.

Roaming

When a device is roaming in the same device mobility group, Cisco Unified Communications Manager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the CFA CSS gets set to None, and the CFA CSS Activation Policy gets set to With Activating Device/Line CSS, then:

- The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.
- If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS get used as the CFA CSS.
- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.

GUI Changes

- In release 6.0, access device mobility groups and device mobility information under the System menu (**System > Device Mobility > Device Mobility Group** and **System > Device Mobility > Device Mobility Information**)
- The added Location Configuration window supports Device Mobility. Access this window under the System menu (**System > Location**).

Where to Find More Information

- Cisco Unified Communications Manager Device Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(1)*
- For more information about configuration options for Call Forward All, see the Directory Number Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*, and the Understanding Directory Numbers chapter in the *Cisco Unified Communications Manager System Guide*.

Directed Call Park

Directed Call Park, introduced in Cisco Unified Communications Manager Release 4.2(1), allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Directed Call Park Configuration window. Configured directed call park numbers exist cluster wide. You can configure phones that support the directed call park Busy Lamp Field (BLF) button to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF button to speed dial a directed call park number.

A user can retrieve a parked call by dialing a configured retrieval prefix followed by the directed call park number where the call is parked.

Note Cisco recommends that you treat Call Park (a hold function) and Directed Call Park (a transfer function) as mutually exclusive: enable one or the other, but not both. If you do enable both, ensure that the numbers that are assigned to each are exclusive and do not overlap.

GUI Changes

- In release 6.0, access directed call park from the Call Routing menu (**Call Routing > Directed Call Park**).

Where to Find More Information

- Call Park and Directed Call Park, *Cisco Unified Communications Manager Features and Services Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(1)*
- Advanced Call Handling, phone user guides

Do Not Disturb

The Do Not Disturb (DND) feature allows you to turn off the ringer for an incoming call. When DND is enabled, you can also choose to have the Cisco Unified IP Phone beep or flash to indicate an incoming call. Users can configure DND directly from their Cisco Unified IP Phone or from the User Options.

With DND enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls or calls with Multi-Level Precedence & Preemption (MLPP), will ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

Although DND prevents most incoming calls from ringing on a phone, the following features can override DND:

- Park reversion—For a locally parked call, park reversion overrides DND.
- Pickup—For locally placed pickup requests, pickup overrides DND.
- Hold reversion and intercom—Both hold reversion and intercom override DND, and the incoming call gets presented normally.
- MLPP and CER—Both MLPP and CER calls override DND and cause the phone to ring.
- Callback—Callback overrides DND, and callback notification still gets presented to the user.
- Pickup notification—When you enable DND Ringer Off, the user only receives visual pickup notification.
- Hunt list—When you enable DND on a phone in a hunt list, a call to the hunt list still gets presented to that phone.

Note Keep in mind that hunt list calls still get presented when DND Ringer Off is enabled by using DND alert settings. The hunt list call will not override DND.

Cisco Unified Communications Manager Administration Configuration Tips

To configure DND, complete the following tasks:

1. Configure DND service parameters (**System > Service Parameters**).
2. Configure DND softkeys (**Device > Device Settings > Softkey Template**).

3. Configure DND feature line keys (**Device > Phone**).

Note Depending on your system, you can configure either DND softkeys or DND feature line keys, or you can configure both.

4. Configure device-based DND parameters (**Device > Phone**).
5. Configure phone profile settings (**Device > Device Settings > Common Phone Profile**).

When you configure DND, keep the following configuration tips in mind:

- Be aware that Cisco Unified Communications Manager provides one system-wide service parameter for do not disturb: BLF Status Depicts DND. This parameter determines whether DND status is considered in the Busy Lamp Field (BLF) status calculation.
- You can configure DND on a per-device basis or in the common phone profile. If you do not set up DND at the device level, the common phone profile settings get used.

GUI Changes

For DND, Cisco Unified Communications Manager Administration includes one new service parameter, a DND softkey on the softkey template, as well as new fields on the Phone Configuration window and the Common Phone Profiles window.

To set the new service parameter, navigate to **System > Service Parameters** and choose the appropriate server and the Cisco CallManager service. You can specify either True or False for the BLF Status Depicts DND parameter.

To configure device parameters for DND, choose **Device > Phone** and configure the following parameters:

- Do Not Disturb
- DND Option
- DND Incoming Call Alert

To configure common phone profiles for DND, choose **Device > Device Settings > Common Phone Profile** and set the following parameters:

- DND Option
- DND Incoming Call Alert

To add a DND softkey, choose **Device > Phone > Softkey Template**. You can add a DND softkey for use in the following states:

- Connected
- Connected Conference
- Connected Transfer
- Off Hook
- Off Hook with Feature
- On Hold
- Remote In Use
- On Hook

To add a feature line key, choose **Device > Device Settings > Phone Button Template** and add Do Not Disturb in the Phone Button Template Configuration window.

Service Parameters

- BLF Status Depicts DND—Specifies True or False.

User Tips

Users activate do not disturb (DND) by using any of the following options:

- Softkey
- Feature line key
- Cisco Unified Communications Manager User Options

After you activate DND, the phone status line displays **Do not disturb is active**, the DND line button icon becomes an empty circle, and the lamp turns amber if the DND feature line key is configured.

Cisco Unified Communications Manager 6.0.supports a subset of Do Not Disturb that is called Do Not Ring. Do Not Ring allows the user to toggle a Do Not Disturb state on/off for a device by using a feature key or softkey.

Note The feature key does not apply to the Cisco Unified IP Phone 7911G or 7906G.

Do Not Disturb disables all visual and audible notification of an incoming call during the ring-in state. Do Not Ring only allows the user to turn off the audible ring during the ringing-in state.

Supported Cisco Unified IP Phones (SCCP and SIP):
7971G-GE, 7970G, 7961G-GE, 7961G, 7941G-GE, 7941G, 7911G, 7906G

Supported Cisco Unified IP Phones (SCCP only):
7960G and 7940G (both softkey only) and 7931G

BAT Considerations

You can use the Bulk Administration Tool (BAT) to configure DND for groups of users. The BAT phone template includes the following DND fields:

- Do Not Disturb check box
- DND Incoming Call Alert

Where to Find More Information

- Do Not Disturb, *Cisco Unified Communications Manager Features and Services Guide*
- Common Phone Profile Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Softkey Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Phone Template, *Cisco Unified Communications Manager Bulk Administration Guide*

Hold Reversion

The Hold Reversion feature, which was introduced in Cisco Unified Communications Manager Release 4.2(3), alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

For example, if you configure this feature to notify you when a call remains on hold past 30 seconds, Cisco Unified Communications Manager sends an alert, such as a ring or beep, to the phone after 30 seconds. You can also configure reminder alerts at configured intervals. A user can retrieve a reverted call on hold by going off hook, which deactivates the feature.

Where to Find More Information

- Hold Reversion, *Cisco Unified Communications Manager Features and Services Guide*
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*
- The Cisco Unified IP Phone administration guides for Cisco Unified IP Phones that support hold reversion and this version of Cisco Unified Communications Manager
- *Cisco Unified IP Phone User Guides*
- Release Notes for Cisco Unified Communications Manager Release 4.2(3)

Intercom

The Intercom feature allows a user to place a call to a predefined target (phone). The called destination auto-answers the call in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless of whether the called party is busy or idle.

To ensure that the voice of the called party is not sent back to the caller when the intercom call is automatically answered, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom provides only one-way audio from the caller to the called party. The called party must manually press a key to talk to the caller.

Note Intercom does not support Cisco Extension Mobility.

Cisco Unified Communications Manager Administration Configuration Tips

1. Create intercom partition (**Call Routing > Intercom > Intercom Route Partition**). When you create an intercom partition, Cisco Unified Communications Manager Administration automatically generates a corresponding intercom calling search space with the same name and includes the intercom partition. See Intercom Partition Configuration in the *Cisco Unified Communications Manager Administration Guide*.
2. Create intercom calling search space (**Call Routing > Intercom > Intercom Calling Search Space**). When you create an intercom partition, Cisco Unified Communications Manager Administration automatically generates a corresponding intercom calling search space with the same name and includes the intercom partition. However, if you need to create a intercom calling search space other than the one that is generated automatically when you create the intercom partition, use these menus. See Intercom Calling Search Space Configuration in the *Cisco Unified Communications Manager Administration Guide.*
3. Create intercom translation pattern (**Call Routing > Intercom > Intercom Translation Pattern**). (This step is optional.) See Intercom Calling Translation Pattern Configuration in the *Cisco Unified Communications Manager Administration Guide.*
4. Create intercom directory number (**Call Routing > Intercom > Intercom Directory Number**). See Intercom Directory Number Configuration in the *Cisco Unified Communications Manager Administration Guide.*

5. Add the intercom button to the appropriate phone button template (**Device > Device Settings > Phone Button Template**). See Phone Button Template Configuration in the *Cisco Unified Communications Manager Administration Guide.*
6. Assign intercom DN to a phone (**Device > Phone > Add New**). After completing the device information, click the line to which intercom gets configured. See Directory Number Configuration and Cisco Unified IP Phones Configuration in the *Cisco Unified Communications Manager Administration Guide.*

GUI Changes

- You configure Intercom by using the four new Cisco Unified Communications Manager configuration windows that are provided from **Call Routing > Intercom.**
  - Intercom Route Partition
  - Intercom Calling Search Space
  - Intercom Directory Number
  - Intercom Translation Pattern
- New Intercom link on the Phone Configuration window, Association Information pane.
- New Intercom button on the Phone Button Template Configuration window.

User Tips

The system administrator configures Intercom in Cisco Unified Communications Manager Administration. The system administrator configures programmable buttons

- To directly dial someone's intercom line and/or
- To begin an intercom call, so the user can enter a specific intercom number to complete this call.

The intercom recipient can

- Listen to the intercom caller audio without answering
- End the call at any time by invoking the End Call softkey, or
- Press the intercom button to speak to the intercom caller.

Supported Cisco Unified IP Phones (SCCP and SIP):
7971G-GE, 7970G, 7961G-GE, 7961G, 7941G-GE, 7941G

Supported Cisco Unified IP Phones (SCCP only):
7931G, 7914 Expansion Module

BAT Considerations

The Cisco Unified Communications Manager administrator can use the Bulk Administration Tool (BAT) to add many intercom users at once instead of adding users individually. Refer to the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

Security Considerations

An intercom call represents a separate call and does not have media mixing to be played to third party. Basic call security should already cover all cases for intercom calls.

CTI Considerations

CTI supports both speakerphone and headset options for intercom as well as auto-answer settings for intercom lines.

Where to Find More Information

- Intercom Partition Configuration, *Cisco Unified Communications Manager Administration Guide*
- Intercom Directory Number Configuration, *Cisco Unified Communications Manager Administration Guide*
- Intercom Calling Search Space, *Cisco Unified Communications Manager Administration Guide*
- Intercom Translation Pattern Configuration, *Cisco Unified Communications Manager Administration Guide*
- Phone Button Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified Communications Manager Intercom, *Cisco Unified Communications Manager Features and Services Guide*

Licensing Enhancements

Use licensing in Cisco Unified Communications Manager Administration to accurately track the number of devices that are connected to Cisco Unified Communications Manager, including third-party SIP phones, and compare it with the number of unit licenses that have been purchased.

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of IP phones. Using the Licensing Configuration window in Cisco Unified Communications Manager Administration, administrators can manage the phone and node licenses that get purchased and used.

The system generates licenses for requested Cisco Unified Communications Manager nodes (servers in a Cisco Unified Communications Manager cluster) and the phones that are associated with those nodes. Two types of licenses exist: production licenses and starter licenses. Production licenses for Cisco Unified Communications Manager represent licenses for phones and nodes that are purchased from Cisco. Starter licenses get replaced when a production license file is uploaded.

Cisco Unified Communications Manager keeps track of the software license version. Each time that the Cisco CallManager service restarts, this version check gets performed. If Cisco Unified Communications Manager fails to load (for example, because the license file is missing), the Service Manager tries to restart the Cisco CallManager service three times. At each attempt to restart, the license file check gets performed, and an alarm gets written to syslog.

The software license version displays in the License Unit Report window of Cisco Unified Communications Manager Administration. See License Unit Report, in the *Cisco Unified Communications Manager Administration Guide*.

Note For convenience, customers get an additional 5 percent of their total licenses when they receive their initial licenses.

Starter Licenses

Cisco Unified Communications Manager comes preinstalled with starter licenses, so a file upload is not required. Starter licenses have no expiration date and are available in limited quantities. Be aware that starter licenses are only available for fresh installations; they are not available for upgrades or migrations from previous releases. Starter licenses support only one Cisco Unified Communications Manager node and up to 50 device license units.

Starter license units get replaced when you purchase a production license.

Licenses for Primary Devices

Each phone type requires a fixed number of device license units. For example, Cisco Unified IP Wireless Phone 7920 requires four device license units, and Cisco Unified IP Phone 7970 requires five device license units. If you want licenses for four 7920 phones and four 7970 phones, you require 36 device license units. Additionally, certain types of applications, such as IP Communicator or mobility voice access, consume device license units.

Licenses for Adjunct Devices (Applications)

Certain types of applications, such as Cisco IP Communicator, Cisco Unified Mobile Communicator, and Cisco Unified Personal Communicator, consume device license units. For example, if IP communicator gets configured as a primary device to an end user, it consumes three device license units. If it gets configured as an adjunct device (by choice of a phone in the Primary Phone field in Phone Configuration), it consumes one device license unit, and the license unit calculator window displays the units that are consumed as Cisco IP Communicator (Adjunct).

Licenses for Mobility End User

When you configure an end user to have mobility functionality (check the Enable Mobility check box on the End User Configuration window), two device license units get consumed. When you uncheck the Enable Mobility check box, the two device license units get set back to zero.

To determine the number of units of licenses that are required for each phone and application, see Calculating License Units in the *Cisco Unified Communications Manager Administration Guide*.

Cisco Unified Communications Manager Administration Configuration Tips

See the following migration and upgrading configuration tips.

Migrating from Cisco Unified Communications Manager 4.2(3) to 6.0(1)

When you migrate from Cisco Unified Communications Manager Release 4.2(3) to 6.0(1), the licenses that are required for existing phones and existing Cisco Unified Communications Manager nodes are calculated, and an intermediate file (XML file) that contains these license counts will get generated during the Cisco Unified Communications Manager migration process. Cisco gives these licenses free of cost because you are already using these phones for Cisco Unified Communications Manager Release 4.2(3). If you are adding new phones and nodes after migrating to Cisco Unified Communications Manager Release 6.0(1), you need to paste the intermediate license file in the License Registration window that is on CCO. See the *Upgrading Cisco Unified Communications Manager* and the *Data Migration Assistant User Guide* for more information.

Upgrading to Cisco Unified Communications Manager Release 6.0(1)

To successfully upgrade to release 6.0(1), perform the following steps:

1. Obtain the license file for release 6.0(1) (see Obtaining a License File, in the *Cisco Unified Communications Manager Administration Guide*).
2. Upgrade to Cisco Unified Communications Manager 6.0(1). (See the *Upgrading Cisco Unified Communications Manager Release 6.0(1)*.)

Note The Cisco CallManager service will not activate due to lack of licenses. An alarm and alert get generated (see the Syslog for information).

3. After the upgrade, upload the appropriate license file (that you obtained in the previous step). See Uploading a License File, in the *Cisco Unified Communications Manager Administration Guide* for information on obtaining the appropriate license file.
4. Using Cisco Unified Serviceability, restart the Cisco CallManager service.

GUI Changes

- **Licensing > License Unit Report**—Displays Software License Version
- **Licensing > License Unit Calculator**—New device types (phones, nodes, and applications)

Serviceability Considerations

- If Cisco Unified Communications Manager does not have the appropriate license file, a Real-Time Monitoring Tool (RTMT) alert gets generated. See the *Cisco Unified Serviceability Administration Guide* for more information on alarms, and see the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* for more information on alerts.
- Cisco Unified Communications Manager keeps track of the software license version. Each time the Cisco CallManager service restarts, this version check gets performed. If Cisco Unified Communications Manager fails to load (for example, because the license file is missing), the Service Manager tries to restart the Cisco CallManager service three times. At each attempt to restart, the license file check gets performed, and an alarm is written to syslog.

Where to Find More Information

- Licensing, *Cisco Unified Communications Manager System Guide*
- License Unit Report, *Cisco Unified Communications Manager Administration Guide*
- License Unit Calculator, *Cisco Unified Communications Manager Administration Guide*
- License File Upload, *Cisco Unified Communications Manager Administration Guide*
- Licensing for Third-Party SIP Phones, *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*

Log Out of Hunt Groups

The Log Out of Hunt Groups feature, which was introduced in Cisco Unified Communications Manager Release 4.2(1), allows phone users to log out their phones from receiving calls that get routed to directory numbers that belong to line groups to which the phone lines are associated. Regardless of the phone status, the phone rings normally for incoming calls that are not calls to the line group(s) that are associated with the phone. The phone provides a visual status of the login state, so the user can determine by looking at the phone whether they are logged in to their line group(s).

Where to Find More Information

- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Softkey Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Advanced Call Handling, phone user guides
- *Release Notes for Cisco Unified Communications Manager Release 4.2(1)*

MGCP T.38 Enhancements

Introduced in Cisco Unified Communications Manager release 4.2(3), T.38 fax relay added the following support (see Table 3):

- Cisco Unified Communications Manager supports CA-controlled MGCP T.38 fax relay.
- Fax calls use T.38 in CA-controlled mode if IOS enables T.38 (default).
- Fax calls use fax passthrough (or Cisco fax relay) if IOS disables T.38 (transparent to Cisco Unified Communications Manager).
- Both H.323 and MGCP (IOS only) support T.38 fax relay. For T.38 fax relay interworking between H.323 gateways and MGCP gateways, ensure MGCP gateways are configured to operate in CA-controlled mode.

Note Cisco Unified Communications Manager Release 5.0 does not include features from release 4.2(3). Release 6.0 includes those features.

In release 5.0, T.38 fax relay introduced the following support:

- SIP support through the SIP Trunk (configured by using SIP Trunk Configuration)
- H.323 and SIP T.38 interoperability

In release 6.0, T.38 fax relay added the following support:

- T.38 interoperability support between SIP and MGCP

T

Table 3 T.38 Enhancements for Cisco Unified Communications Manager

T.38 Enhancement	Cisco Unified Communications Manager Release 4.1(1)	Cisco Unified Communications Manager Release 4.2(3)	Cisco Unified Communications Manager Release 5.0(1)	Cisco Unified Communications Manager Release 6.0(1)
T.38 supports H.323.	Yes	Yes	Yes	Yes
T.38 supports MGCP and H.323.	No	Yes	No	Yes
T.38 supports H.323 and SIP.	No	No	Yes	Yes
T.38 supports H.323, SIP, and MGCP.	No	No	No	Yes

Where to Find More Information

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*
- *Cisco IOS Fax and Modem Services over IP Application Guide*

Overlap Sending and Receiving for H.323 Gateways

Introduced in Cisco Unified Communications Manager Release 4.2(1), support exists for overlap sending and receiving for H.323 gateways. H.323 module users do not need to dial all the digits for the setup message to be sent to an H.323 device. You can enable the overlap sending feature for the

individual route pattern by using the Allow Overlap Sending check box on the Route Plan Configuration window. To enable the overlap receiving feature, you must set the Cisco CallManager service parameter, Overlap Receiving Flag for H.323, to True.

Where to Find More Information

- Client Matter Codes and Forced Authorization Codes, *Cisco Unified Communications Manager Features and Services Guide*

Privacy on Hold

With the privacy on hold feature, administrators can enable or disable the capability of users with phones that share the same line (DN) to view call status and retrieve calls on hold.

Administrators enable or disable privacy on hold for all phones in the cluster. To enable privacy on hold, the administrator must also enable the privacy feature for the phone or for all phones. Privacy on hold activates automatically on all private calls when privacy on hold is enabled.

To activate privacy on hold, users press the Hold softkey while on a private call. To return to the call, users press the Resume softkey. The phone that put the call on hold displays the status indicator for a held call; shared lines display the status indicators for a private and held call.

For more information about configuring and using privacy on hold, refer to the Barge and Privacy chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Programmable Line Keys

Cisco Unified IP Phones support line buttons (the buttons to the right of the display), which are used to initiate, answer, or switch to a call on a particular line. A limited number of features, such as speed dial, extension mobility, privacy, BLF speed dial, DND, and Service URLs, get assigned to these buttons.

The Programmable Line Key (PLK) feature expands the list of features that can be assigned to the line buttons to include features that are normally controlled by softkeys; for example, New Call, Call Back, End Call, and Forward All. When you configure these features on the line buttons, they always remain visible, so you can have a “hard” New Call key.

Cisco Unified Communications Manager Administration Configuration Tips

- Use the Phone Button Template Configuration window to assign programmable line keys.
- After configuring the phone button template, you must assign the phone button template to the phone by using Phone Configuration (reset is required).

GUI Changes

- You can configure the following features on the phone buttons by using Phone Button Template Configuration:
  - Redial (7931 uses existing line button)
  - Speed Dial
  - Hold (7931 uses existing line button)
  - Transfer (7931 uses existing line button)
  - Forward All
  - Line
  - Privacy

  - Service URL
  - Speed Dial BLF
  - Call Park BLF
  - Intercom
  - Malicious Call ID
  - Meet Me Conference
  - Conference
  - Call Park
  - Call Pickup
  - Group Call Pickup
  - Mobility
  - Do Not Disturb
  - Conference List
  - Remove Last Participant
  - Quality Reporting Tool
  - Call Back
  - Other Pickup
  - Video Mode
  - New Call
  - End Call
  - Hunt Group Logout
  - Settings (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Services (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Directories (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Messages (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Information (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Application Menu (7971, 7970, 7961, 7941, and 7914 use existing button)
  - Headset (7971, 7970, 7961, 7941, and 7914 use existing button)
  - None

User Tips

- Supports Cisco Unified IP Phones 7971, 7970, 7961, 7941, 7931 (SCCP only), and 7914 (SCCP only)

BAT Considerations

- The Phone Template supports Phone Button Template Configuration.

Where to Find More Information

- Cisco Unified IP Phone, *Cisco Unified Communications Manager System Guide*

- Phone Button Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*

SCCP Optimization

Cisco Unified Communications Manager Release 4.2(3) introduced this feature. Because this feature consumes resources, ensure this feature gets enabled only when you are getting signaling delays for SCCP phones. Most users do not require this option.

Cisco Unified Communications Manager sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires.

Note For Cisco Unified IP Phones 7960G and 7940G, the firmware version that supports improved SCCP messaging specifies 8.0(2).

In SCCP Version 9, SCCP message structures get altered to allow variable- length messages instead of a fixed-length character array that consumes bandwidth.

Where to Find More Information

- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(3)*

SDL Traces

Since it was introduced in Cisco Unified Communications Manager Release 4.2(1), you can use the Asynchronous SDL Logging Enabled parameter to determine whether Cisco Unified Communications Manager logs SDL traces in asynchronous mode. Asynchronous mode allows Cisco Unified Communications Manager to manage SDL trace data independently from other call-processing activities, which can improve Cisco Unified Communications Manager performance. This parameter setting does not affect SDL trace output; only the internal method data gathering is affected. In the event of a Cisco Unified Communications Manager exe crash, the SDL trace may not get fully logged. If asynchronous logging is enabled, an exception handler gets called to ensure that all the SDL trace data that were collected up until the time of crash get fully logged.

Where to Find More Information

- Trace, *Cisco Unified Serviceability Administration Guide*

SIP Endpoints Support

The following features support SIP endpoints in release 6.0.

- Directed Call Park (see the "Directed Call Park" section on page 38)
- Log Out of Hunt Groups (see the "Log Out of Hunt Groups" section on page 46)
- Conference Chaining (for ad hoc conferences) (see the "Advanced Ad Hoc Conference" section on page 28)

- Voice Quality Metrics (see the "Call Diagnostics and Voice Quality Metrics" section on page 30)
- Call Pickup Group (see the "Call Pickup Notification" section on page 33)
- Hold Reversion (see the "Hold Reversion" section on page 41)
- Cisco Unified Communications Manager Assistant (see the "Cisco Unified Communications Manager Assistant" section on page 58)
- CTI enhancements (see the "CTI Enhancements" section on page 36)
- Call Select
- Privacy (see the "Privacy on Hold" section on page 48)
- Line-based Message Waiting Indicator
- Hunt Group CDR (see the "Call Detail Record Definitions" section on page 81)

Cisco Unified Communications Manager Administration Configuration Tips

- Directed Call Park—If reversion number is not configured, the call reverts to the parker (parking party) after the call park reversion timer expires. Directed Call Park for SIP phones design incorporates busy lamp field (BLF) plus call transfer (to a park code). The transfer functionality remains the same as for SCCP phones. Directed Call Park for SIP phones includes the following limitations:
  - Invoke directed call park by using the transfer softkey on Cisco Unified IP Phone Models 7940 and 7960 that are using SIP.
  - The system does not support directed call park when the blind transfer softkey is used on Cisco Unified IP Phone Models 7940 and 7960 that are using SIP.
  - The system does not support directed call park BLF on Cisco Unified IP Phone Models 7940 and 7960 that are using SIP and third-party SIP phones.
  - The following Cisco Unified IP Phones that are using SIP support directed call park BLF: 7941, 7961, 7970, and 7971.
- Conference Chaining—You can invoke ad hoc conference chaining for SIP phones by using the Conference and Transfer functions. The system does not support Direct Transfer and Join. Supported Cisco Unified IP Phones Models include 7911, 7941, 7961, 7970, and 7971 that are using SIP.
- Log Out of Hunt Groups—This feature presents the following limitations:
  - When Cisco Unified IP Phone Models 7906, 7911, 7941, 7961, 7970, and 7971 that are using SIP are logged in to hunt groups, and Call Forward All is activated, the call gets presented to the SIP phone.
  - When Cisco Unified IP Phone Models 7940 and 7960 that are using SIP are logged in to hunt groups, and Call Forward All is activated, the phone will get skipped, and the next phone in the line group will get rung.
  - You can log Cisco Unified IP Phone Models 7940 and 7960 that are using SIP and third-party SIP into/out of hunt groups by using the Phone Configuration window, but no softkey support exists.
  - Cisco Unified IP Phone Models 7940 and 7960 that are using SIP and third-party SIP phones will not show "Logged out of hunt groups" on the status line.
  - Cisco Unified IP Phone Models 7940 and 7960 that are using SIP and third-party SIP phones will not play the hunt group logoff notification tone regardless of whether the tone is configured.

- Voice Quality Metrics—Fully supported by Cisco Unified IP Phone Models 7911, 7941, 7961, 7970, and 7971 that are running SIP, support includes end-of-call reporting, mid-call reporting (for example, call hold, media disconnect), and voice quality metrics. Cisco Unified IP Phone Models 7905, 7912, 7940, and 7960 that are using SIP do not report voice quality metrics or mid-call reporting. To enable voice quality metrics on Cisco Unified IP Phones using SIP, check the Call Stats check box on the SIP Profile Configuration window.
- Call Pickup Group—This feature reflects the following limitations:
  - Call pickup notification, audio, and visual alert supports Cisco Unified IP Phones (SIP) 7911, 7941, 7961, 7970, and 7971.
  - Call pickup notification, audio, and visual alert do not get supported on Cisco Unified IP Phones (SIP) 7905, 7912, 7940, and 7960.
  - Call pickup notification, audio, and visual alert only supports licensed third-party SIP phones.
- Hold Reversion—Call focus priority gets sent to the SIP phone by its TFTP configuration file. The Cisco Unified IP Phones (SIP) 7906, 7911, 7941, 7961, 7970, and 7971 support the Hold Reversion feature. (This capability requires version 8.3(1) phone firmware.)
- Call Select and Privacy—Release 4.2 provides Call Select and Privacy enhancements for SCCP phones that use shared lines. Releases 5.0 and 6.0 provide the same enhancements for SIP phones that use shared lines. The system does not support Select and Privacy on nonshared lines for SIP phones.
- Line-based Message Waiting Indicator—Release 6.0 provides line-based message waiting indicator for SIP phones.

GUI Changes

See the individual features that this document lists for a list of GUI changes.

Serviceability Considerations

See the individual features that this document lists for a list of Serviceability changes.

BAT Considerations

See the individual features that this document lists for a list of BAT changes.

CAR/CDR Considerations

See the individual features that this document lists for a list of CAR changes.

Security Considerations

See the individual features that this document lists for a list of security changes.

CTI Considerations

See the individual features that this document lists for a list of CTI changes. Also see the "CTI Enhancements" section on page 36.

Features that CTI Does Support on SIP Phones

CTI on SIP phones supports the following features:

- Set lamp mode
- Display text on device
- Device-based, application-controlled softkeys

- Play device tone
- Ringing notification
- Call Park/Unpark – Request to park/unpark a specified call
- Call Park Reminder
- Call Privacy Change Notification
- Line Ringer Override – Overrides the current ringer setting for the specified line

Note Cisco Unified IP Phones (SIP) that are configured to use User Datagram Protocol (UDP) as the transport mode (instead of TCP) will not support the device data passthrough functionality; for example, the Quality Reporting Tool (QRT) requires the data passthrough functionality, so it cannot be used with IP phones that are configured with UDP.

Where to Find More Information

- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- SIP Profile Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Computer Telephony Integration, *Cisco Unified Communications Manager System Guide*

SIP Third-Party Phones Enhancements

Cisco Unified Communications Manager Release 6.0 supports Cisco Unified IP Phones (SIP) in addition to SIP phones that third-party companies design to work with Cisco Unified Communications Manager.

Licensing for Third-Party SIP Phones

Third-party SIP phones licensing enforces the following limitations:

- Third-party SIP Device (Basic)—Video calls do not get supported. Video enforcement occurs as part of the offer/answer process. If video-related media is provided as part of an offer or answer from a SIP device that is not permitted to negotiate video, only the non-video-related parts of the call get extended to the destination party. Similarly, a SIP endpoint that is not permitted to negotiate media will not receive any video-related media in the SDP that is sent from Cisco Unified Communications Manager.
- Third-party SIP Device (Advanced) and (Basic)—Cisco-specific SIP extensions do not get supported. Some Cisco-specific SIP extensions that do not get supported include service URIs, header extensions, dialog subscriptions, and remote call control proprietary mime types. Cisco Unified Communications Manager will reject any request from a SIP phone that is not permitted to use an advanced feature that uses a service request URI (such as Call Pickup URI, Meet Me Service URI). The SIP profile specifies service URIs. The profile gets assigned to SIP devices. Cisco Unified Communications Manager will block features that require the use of Cisco-specific SIP extensions.

Note Be aware that any wireless third-party SIP client or device must be configured as a Third-Party SIP Device (Advanced) in conformance with Cisco Unified Communications Manager licensing policy.

Cisco Unified Communications Manager Administration Configuration Tips

Administrators use the following Cisco Unified Communications Manager Administration windows to configure third-party SIP phones:

- To configure licensing for third-party SIP phones, choose **Licensing > License Unit Calculator** and **Licensing > License File Upload**.

User Tips

The third-party vendor documentation provides all user information.

Where to Find More Information

- Configuring Non-Cisco SIP Phones, *Cisco Unified Communications Manager Administration Guide*
- License File Upload, *Cisco Unified Communications Manager Administration Guide*
- License Unit Calculator, *Cisco Unified Communications Manager Administration Guide*
- Licensing, *Cisco Unified Communications Manager System Guide*
- For more information about Cisco SIP Extensions, contact your Cisco representative.

SIP Trunk Enhancements

Cisco Unified Communications Manager Release 6.0 provides the following enhancements to SIP trunk:

- AAC/iLBC Voice Codec—See the "AAC/iLBC Voice Codec Support" section on page 27.
- SIP PUBLISH—This feature provides the preferred mechanism for Cisco Unified Communications Manager Release 6.0 to send IP phone presence information to Cisco Unified Presence (CUP) Release 6.0 over a SIP trunk because it provides improved performance. PUBLISH also provides presence information on a line basis; for example, for do not disturb and mobility. Only outbound PUBLISH gets supported. (Cisco Unified Communications Manager Release 5.0 and 6.0 both support SUBSCRIBE/NOTIFY for presence. In addition, Cisco Unity Presence release 6.0 supports both Cisco Unified Communications Manager Release 5.0 and 6.0.)

Cisco Unified Communications Manager Administration Configuration Tips for PUBLISH

The following configuration tips apply to Cisco Unified Communications Manager Administration when configuring a SIP trunk for PUBLISH:

- From the SIP Trunk Configuration window, configure a SIP trunk to access Cisco Unified Presence (destination address). In the destination port field, enter 5070 (preferred port for PUBLISH).
- From the Service Parameters Configuration window for the Cisco CallManager service, in the CUP PUBLISH Trunk field, choose the SIP trunk that you configured.
- Configure a Cisco Unified Presence end user (**User Management > End User Configuration**) and assign a licensing unit to the user (**System > Licensing > Capabilities Assignment**).
- Associate the end user with the line appearance (**Device > Phone Configuration**). From the Phone Configuration window, click the DN that the user will use to access Cisco Unified Presence. Click the Associated End Users button. From the Find and List Users window, choose an end user that will access Cisco Unified Presence.
- DND Support for SIP Trunk PUBLISH—Because DND is device based in release 6.0, if a device is changed to the DND state, all Cisco Unity Presence-enabled line appearances that are associated with this device could get published. When a device gets changed to the DND state, DND as well as the busy/idle status will get published together to give Cisco Unity Presence more flexibility to process the data.

For Cisco Unity Presence users, consider DND an overall status of the person, rather than just a device setting; therefore, when DND is activated from a device, all line appearances that are associated with that device get published with the DND state, if the line appearances are associated with a Cisco Unity Presence user. As a result, DND will also get set on IP phone messenger (IPPM) and would block instant messages (IMs) on the IPPM device. It will also set DND on any other device that is associated with the user (unless a line appearance exists on that device that is associated with multiple users). The setting does not block Cisco Unity PresenceCommunicator IM or affect the display on Cisco Unity PresenceCommunicator in this release. For more information, see the Cisco Unified Presence documentation at cisco.com.

- Shared Lines—If Phone A and Phone B are sharing DN 1000, when a user picks up Phone A and makes a call on the line 1000, Cisco Unified Communications Manager notifies Cisco Unity Presence that line 1000 is busy. This information gives the watcher the illusion that all lines for DN 1000 are busy. This does not represent accurate information because line 1000 on Phone B remains idle. Cisco Unified Communications Manager tells Cisco Unity Presence that line 1000 on Phone A is busy. In release 6.0, Cisco Unified Communications Manager publishes by line appearance. The system considers a line appearance a (DN, Device) pair.
- Multiple Partitions—When Cisco Unified Communications Manager publishes the presence status of a DN, it also shows the partition in which the DN is associated.
- Associating Username—With shared line and multiple partitions supported, Cisco Unity Presence cannot assume that it works only with one DN for each phone and also one partition across the whole Cisco Unified Communications Manager system. In release 6.0, a line appearance can associate with an end user. SIP trunk will publish the status of the line appearance on behalf of the end user that is associated with that line appearance, which means it can get used to identify Cisco Unity Presence-enabled lines. If a line appearance is associated with an end user, the systems consider it as Cisco Unity Presence -enabled; therefore, its presence information will get published.

Service Parameter Changes for PUBLISH

This release adds the following Cisco CallManager service parameters to the Service Parameter Configuration window:

- CUP PUBLISH Trunk
- Default PUBLISH Expiration Timer
- Minimum PUBLISH Expiration Timer
- Retry Count for SIP Publish
- SIP Publish Timer

Serviceability Considerations

Cisco Unified Serviceability collects and displays the following PUBLISH-related performance counters:

- SIP_StatsPublishIns
- SIP_StatsPublishOuts
- SIP_StatsRetryPublishOuts
- SIP_StatsRetryRequestsOut

The following performance counters exist in Cisco Unified Communications Manager Release 5.0, but the PUBLISH feature impacts their values:

- SIP_SummTotalOutReq
- SIP_SummTotalInRes

- SIP_StatsRetryRequestsOut

Security Considerations

- RFC 3903 suggests the use of TLS and digest authentication against issues such as Access Control, Denial of Service Attacks, Replay Attacks, and Man in the Middle Attacks. Because Cisco Unified Communications Manager and Cisco Unified Presence support TLS and digest authentication, no changes occur in Release 6.0. The administrator can configure and enable TLS and digest authentication for Cisco Unified Communications Manager and Cisco Unified Presence. Additionally, IPSec can get used as an alternative to TLS.

BAT Considerations

- BAT provides a tool that examines all Cisco Unity Presence licensed users and their primary extensions and associated device line appearances for users after Cisco Unified Communications Manager is upgraded from 5.x to 6.0. You need this tool during the upgrade/migration of Cisco Unity Presence when connecting to Cisco Unified Communications Manager Release 6.0 (Because all the backend subscriptions get deleted and the new line appearance-based presence need to be available for Cisco Unity Presence users). To perform the migration, BAT uses the Export and Update functions. The export csv format specifies User ID, Device, Directory Number, Partition. The last three columns form a line appearance.
- To access the Export and Update windows, choose **Bulk Administration > Users > Line Appearance > Export Line Appearance** and **Bulk Administration > Users > Line Appearance > Update Line Appearance**.
- The Export and Update windows include a check box, Export Line Appearance for Cisco Unity Presence User Only (and Update Line Appearance for Cisco Unity Presence Users Only). When this check box gets checked, the export or update operation gets performed on the Cisco Unity Presence users. Non-Cisco Unity Presence users will not get exported or updated.

Where to Find More Information

- SIP Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Understanding Session Initiation Protocol, *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Communications Manager Applications

The following sections describe the Cisco Unified Communications Manager 6.0 applications enhancements:

- Cisco Unified Communications Manager Extension Mobility, page 57
- Cisco Unified Communications Manager Assistant, page 58
- Cisco Unified Mobility, page 61
- Migrating from Cisco Unified Mobility to Cisco Unified Communications Manager, page 64
- Multilevel Precedence and Preemption (MLPP) Supplementary Services, page 66
- Multilevel Precedence and Preemption Enhancements, page 67

- Recording and Monitoring, page 68

Cisco Unified Communications Manager Extension Mobility

The Cisco Extension Mobility (EM) equivalency enhancement that was introduced in Cisco Unified Communications Manager Release 4.2 eliminates the phone model dependency of phone button templates. The following factors determine the model equivalency among the various phones:

- Various features that the phone models support
- Number of buttons that the phone models support

The EM equivalency enhancement introduces the following support feature for the Cisco Unified IP Phones:

- Feature Safe on Phone Button Template
  - Phones can use any phone button template that has the same number of buttons that the phone model supports.
  - In Release 6.0 of Cisco Unified Communications Manager Administration, be aware that some Cisco Unified IP Phones (for example, 7970 and 7971) support Feature Safe.

Release 6.0 adds the following enhancements to Cisco Extension Mobility in Cisco Unified Communications Manager Release 6.0:

- After a user logs in to a phone, the Phone Configuration window for that device now reflects the Current End User Profile and Current Device Profile as well as links to the applicable End User Profile and Device Profile Configuration windows. This information displays in the Extension Information portion of the Phone Configuration window.
- When you subscribe Cisco Unified IP Phones to Cisco Extension Mobility, the options for Logout Profile in the Phone Configuration window have changed. You now have the option to select either Use Current Device Setting or any specific configured device profile that has a matching model and protocol type (the drop-down list box lists these device profiles). When total number of items in the drop-down list box exceeds 50, the drop-down list box changes to a search button.
- When you select the Use Current Device Setting option for Logout Profile, this no longer creates an autogenerated device profile. With the extension mobility rearchitecture, the internal implementation changed such that autogenerated device profiles no longer get used. During extension mobility login, the actual device record no longer changes. Instead, a mapping between the login device and the login profile gets created. If the logout profile is something other than Use Current Device Setting, during extension mobility logout, the mapping between the device and the logout profile remains. With the Use Current Device Setting option, no dynamic mapping occurs between the device and the device profile when the device is in the logout state.
- The line number for a phone does not change in the Phone Configuration window when a user logs in to a phone. It continues to display the line number that is associated with the phone when no user is logged in.
- The release makes New Find and List Actively Logged In Devices window available from the Actively Logged In Device Report link in the Related Links drop-down list box in the upper, right corner of the Phone Configuration window.

Service Parameter Changes

The reorganized Extension Mobility section of the Service Parameters Configuration window adds a new Advanced configuration button. Clicking Advanced displays the advanced Extension Mobility service parameters. The Maximum Concurrent Requests service parameter now represents an advanced service parameter. No new service parameters exist for extension mobility for this release.

Where to Find More Information

- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant supports the following enhancements in Cisco Unified Communications Manager Release 6.0:

- Cisco Unified Communications Manager Assistant Configuration Wizard—The release adds the following windows to the configuration wizard:
  - Secondary phone service
  - Intercom partition
- The system provides BAT support for Cisco Unified IP Phones 7940, 7960, and 7970
- Cisco Unified Communications Manager Assistant on the Phone—The assistant can use the physical phone buttons and softkeys to perform most of the call-handling tasks that the assistant can perform by using the assistant console application. Cisco recommends that an assistant use the Cisco Unified Communications Manager Assistant-on-phone features only if that assistant supports no more than five managers.
- Assistant Console Layout—The assistant can customize the size and position of panels in the assistant console. Use the View menu to change the color scheme and font and to refresh initial default settings.
- Cisco Unified Communications Manager Do Not Disturb—Prior to Cisco Unified Communications Manager Release 6.0, Cisco Unified Communications Manager Assistant implemented DND at its layer. In Cisco Unified Communications Manager Release 6.0, DND represents a Cisco Unified Communications Manager feature, so Cisco Unified Communications Manager Assistant no longer uses the DND that it provided. (See the "Do Not Disturb" section on page 39.)
- Cisco Unified Communications Manager Intercom—Prior to Cisco Unified Communications Manager Release 6.0, Cisco Unified Communications Manager Assistant implemented intercom at its layer. In Cisco Unified Communications Manager Release 6.0, intercom represents a Cisco Unified Communications Manager feature, so Cisco Unified Communications Manager Assistant no longer uses its intercom feature for Cisco Unified IP Phones 7941, 7961, 7970, and 7971. (See the "Intercom" section on page 42.)

  Note Cisco Unified IP Phones 7940 and 7960 do not support the Cisco Unified Communications Manager intercom feature. These phones must use the intercom feature that Cisco Unified Communications Manager Assistant provides.

- Alert Tone—Prior to Cisco Unified Communications Manager Release 6.0, the only indication for assistant-handled calls on the manager phone is the call detail that displayed on Status Window. An alert tone helps a manager look at the display and intercept the call. Managers can turn alert tone On/Off from the IP Phone Service Menu on their phone. Assistants can turn alert tone On/Off for their managers from the manager configuration window in the assistant console and assistant phone. The assistant can also toggle the alert tone for their managers from the assistant console My Managers window.
- SIP Phone Support—Managers and assistants can use Cisco Unified IP Phones 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE that are using SIP (session initiated protocol).

- Scalability—This feature enhances the scalability numbers to 3500 managers and 3500 assistants (7000 users). Multiple active Cisco Unified Communications Manager Assistant instances run in the cluster, each managing 2500 users. Three such instances, each running on a separate server with a unique CTI Manager, can exist. To configure this feature, the release adds five new service parameters (see the "New Service Parameters" section on page 60).
- Redirect Softkey—Prior to Cisco Unified Communications Manager Release 6.0, the ImmDiv softkey appeared on the manager and assistant phones. In Cisco Unified Communications Manager Release 6.0, the ImmDiv softkey gets renamed to Redirect.

Cisco Unified Communications Manager Administration Configuration Tips

Cisco Unified Communications Manager Release 6.0 features include the following configuration differences:

- Cisco Unified Communications Manager Assistant Configuration Wizard—You use two windows to configure the Primary Phone Service Name and the Secondary Phone Service Name.
- Cisco Unified Communications Manager Assistant Configuration Wizard—Users use a new window to configure the Cisco Unified Communications Manager Intercom partition, which is required to use the intercom feature with Cisco Unified Communications Manager Assistant.
- The system provides BAT support for Cisco Unified IP Phones 7940, 7960, and 7970—The CSV file specifies these devices. (Prior to Cisco Unified Communications Manager Release 4.2, BAT would reject the record if the CSV file contained any non-7960 device.)
- Cisco Unified Communications Manager Do Not Disturb—This feature gets configured on the phone by using the Phone Configuration window. The phone gets associated to the manager by using the End User Configuration window.
- Cisco Unified Communications Manager Assistant supports the following intercom features:
  - Cisco Unified Communications Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). This intercom feature gets configured by using the DN configuration and end user (manager and assistant) configuration windows.
  - Cisco Unified Communications Manager intercom (used with Cisco Unified IP Phones 7941, 7961, 7970, and 7971). This feature gets configured from the Call Routing menu by using the Intercom Route Partition, Intercom Calling Search Space, Intercom Directory Number, and Intercom Translation Pattern windows. The intercom directory number gets assigned to the device by using the Phone Configuration window. The phone gets associated to the manager or assistant by using the End User Configuration window. On the Assistant Configuration window, choose the incoming intercom line appearance for the assistant from the Intercom Line drop-down list box.
- SIP Phone support—SIP phones get configured in the Phone Configuration window. SIP phones can now be assigned to managers and assistants by using the End User Configuration window.
- Scalability—This enhancement gets configured by using Service Parameters Configuration and End User Configuration. When the service parameters are enabled and configured, the field, Assistant Pool, displays on the Manager Configuration window. From the drop-down list box, choose the applicable pool.

Note If you are migrating from a release previous to Cisco Unified Communications Manager Release 6.0(1), all managers and assistants will migrate to Pool 1 (the default).

- Migration—The following points apply to migration:

  - When Cisco Unified Communications Manager is upgraded from a windows version, all Cisco Unified Communications Manager Assistant manager/assistant configurations migrate. The administrator must run the Data Migration Assistant (DMA) on the Windows platform prior to upgrading the platform to Release 6.0. It creates and exports a DMA tar ball of configuration data to be later installed onto the Release 6.0 platform during an upgrade.
  - When upgrading and migrating from Cisco Unified Communications Manager Release 4.2, you must reinstall the Assistant Console application.

GUI Changes

Cisco Unified Communications Manager Assistant supports the following GUI changes:

- New windows in Cisco Unified Communications Manager Assistant Configuration Wizard for Phone Service Names and Intercom Partition.
- New field, Assistant Pool, on Manager Configuration window for scalability (up to 3500 managers and 3500 assistants).
- The Cisco Unified Communications Manager Assistant iDivert softkey renamed to Redirect (see the Softkey Template Configuration window).

New Service Parameters

- Enable/Disable Multiple Active Mode
- Pool 2: Cisco IPMA Server (Primary) IP Address
- Pool 2: Cisco IPMA Server (Backup) IP Address
- Pool 3: Cisco IPMA Server (Primary) IP Address
- Pool 3: Cisco IPMA Server (Backup) IP Address

User Tips

Cisco Unified Communications Manager Assistant suggests the following end user tips:

- The Cisco Unified Communications Manager Assistant ImmDiv softkey is renamed to Redirect.
- Managers access Do Not Disturb from Cisco Unified Communications Manager softkeys.
- Managers and assistants who use the Cisco Unified IP Phone 7941, 7961, 7970, and 7971 access Intercom from Cisco Unified Communications Manager softkeys.
- The assistant can use the physical phone buttons and softkeys to perform most of the call-handling tasks by using the Assistant Console application.
- The assistant can customize the size and position of panels in the Assistant Console. Use the View menu to change the color scheme and font and to refresh initial default settings.
- Managers can turn alert tone On/Off from the IP Phone Service Menu on their phone. Assistants can turn alert tone On/Off for their managers from the manager configuration window in the assistant console and assistant phone. The assistant can also toggle the alert tone for their managers from the assistant console My Managers window.

BAT Considerations

Cisco Unified Communications Manager Assistant supports the following considerations for BAT, which is now integrated with Cisco Unified Communications Manager Administration.

- The system provides BAT support for Cisco Unified IP Phones 7940, 7960, and 7970

CAR/CDR Considerations

The *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide* documents CDR information for Cisco Unified Communications Manager Assistant.

Where to Find More Information

- Cisco Unified Communications Manager Assistant With Proxy Lines, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Assistant With Shared Lines, *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Mobility

Cisco Unified Communications Manager Release 6.0 integrates the Cisco Unified Mobility features, which include mobile connect and mobile voice access. Mobile connect enables users to manage business calls by using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. mobile voice access extends mobile connect capabilities by way of an integrated voice response (IVR) system that is used to initiate mobile connect calls and activate or deactivate mobile connect capabilities.

Mobile connect and mobile voice access enable flexible management of enterprise and cellular telephone communications and provide these features and benefits:

- Simultaneous desktop ringing—Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset.When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time that a call comes in.
- Desktop call pickup—Users can switch between desktop phone and cellular phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the cellular phone.
- Single enterprise voice mailbox—The enterprise voice mailbox can serve as single, consolidated voice mailbox for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees, and less time is required for users to check multiple voice-messaging systems.
- System remote access—A user cellular phone can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.
- Allowed and blocked access lists—Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (allowed access list) or for which the remote destinations do not ring on an incoming call (blocked access list). Each remote destination presents a cellular or other phone that can be configured to accept transfers from the user desktop phone.
- Caller ID—Caller ID gets preserved and displayed on all calls. Users can take advantage of mobile connect capability with no loss of expected IP phone features.
- Remote on/off control—Users can turn their mobile connect features on or off from the cellular phone by using mobile voice access or from the End User Configuration window.

- Call tracing—Detailed mobile connect calls get logged, which provides information to help the enterprise optimize trunk usage and debug connection problems.
- Security and privacy for mobile connect calls—During an active mobile connect call, the associated desktop IP phone remains secured. Access to the call from the desktop gets eliminated as soon as the cellular connection becomes active, which precludes the possibility of an unauthorized person listening in on the call that is bridged to the cellular phone.
- Mid-call enterprise feature support—You can configure DTMF feature codes as Cisco Unified Communications Manager service parameters: Hold (default equals *81), exclusive hold (default equals *82), resume (default equals *83), transfer (default equals *84), and conference (default equals *85).
- Smartphone support—Users can use the enterprise hold, resume, transfer, conference softkeys on the smartphone in an active call. Users can also enable or disable mobile connect from a smartphone.
- Enterprise feature access for two-stage dialing—You can use enterprise features with two-stage dialing for smartphones. Two-stage dialing allows smartphones to make outgoing calls through Cisco Unified Communications Manager if the smartphone is in business mode. The smartphone dials the Enterprise Feature Access number for Cisco Unified Communications Manager and then dials the destination number.
- Manual handoff calls on dual-mode phone—Dual-mode devices offer an option to manually hand off calls from the PSTN to WLAN and vice versa.

Cisco Unified Communications Manager Administration Configuration Tips

Cisco Unified Mobility supports the following configuration tips:

- To use mobile connect features, you must first disable the Auto Call Pickup feature.
- The Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with mobile voice access. JAVA telephony programming interface (JTAPI) does not support the events that are required for FAC/CMC.
- To support different types of codecs, you must configure a transcoder in Cisco Unified Communications Manager for shared-line CTI ports.
- Mobile connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, the system disables mobile connect features for that call.
- Mobile connect services do not extend to video calls. The cellular phone cannot pick up a video call that is received at the desktop phone.
- Remote destinations must be Time Division Multiplex (TDM) devices.
- Be aware that mobile connect services are available only to directory numbers (DNs) that are in the same partition as the Shared Line CTI User. If the same DN is used in two different partitions, service only extends to the DN in the same partition as the Shared Line CTI User.
- The system does not make CDR Analysis and Reporting (CAR) support available.
- If two or more users share the same extension number, the parameters that are configured on the Line Appearances page correspond to the most recent update. Only one set of parameters gets stored for each extension, whether the extension is shared by multiple users or not.
- Users cannot access Meet-Me feature by using mobile voice access.
- QSIG (Q Signaling) path replacement does not get supported.
- When configuring CTI ports for outgoing calls, make sure the Media Resource group for the CTI Ports does not include Music-On-Hold (MOH) servers.

- When configuring a directory number that is associated with a remote destination profile, you must use ASCII characters only in the Display (Internal Caller ID) field on the Directory Number Configuration window.
- You do not need to configure settings for call forward unregistered, if the end user has configured remote destinations. Appropriate call forwarding will get handled as part of the mobile connect process.

GUI Changes

The release adds new windows for Cisco Unified Mobility configuration:

- **Call Routing > Mobility Configuration**—Contains dual-mode phone handoff settings for call transfers between a user desktop phone and cellular phone.
- **Media Resources > Mobile Voice Access**—Contains settings for localized user IVR prompts.
- **Device > Device Settings > Access Lists**—Determines the phone numbers that are explicitly allowed or blocked for in-progress call transfers.
- **Device > Device Settings > Remote Destination Profile**—Contains the parameters that apply to all the remote destinations (cellular or other phones) that are available for in-progress call transfers and initiation of calls by way of mobile voice access.
- **Device > Device Settings > Remote Destinatio**n—Specifies the cellular (or other phones) that are able to accept transfers from the user desktop phone and can be used to initiate calls by using mobile voice access.

The release updates the following window to support Cisco Unified Mobility configuration:

- **User Management > End User**—New Mobility Information section allows the user to choose remote destination profiles and access lists and enable mobile voice access.

New Service Parameters

These new service parameters support Cisco Unified Mobility:

- Delay before ringing cell phone timer
- Answer too late timer (also known as maximum cell phone ring timer)
- Answer too soon timer (also known as minimum cell phone ring timer)

User Tips

End users can configure mobility by using Cisco Unified Communications Manager User Options:

- **Mobility Settings > Remote destinations**—End users can add their own remote destinations.
- **Mobility Settings > Access lists**—End users can define their own access lists.

BAT Considerations

Cisco Unified Mobility supports BAT, which now integrates with Cisco Unified Communications Manager Administration. The system supports BAT for these functions:

- Users
- Access lists
- Remote destination profiles
- Remote destinations

CAR/CDR Considerations

Be aware that CDR Analysis and Reporting (CAR) support is not available.

Security Considerations

- Be aware that Mobility Voice Access is password-protected.
- During an active mobile connect call, the associated desktop IP phone secured. Access to the call from the desktop gets eliminated as soon as the cellular connection becomes active, which precludes the possibility of an unauthorized person listening in on the call that is bridged to the cellular phone.

Where to Find More Information

- Mobile Connect and Mobile Voice Access, *Cisco Unified Communications Manager Features and Services Guide*
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Migrating from Cisco Unified Mobility to Cisco Unified Communications Manager

This section provides guidelines for migrating Cisco Unified Mobility data to Cisco Unified Communications Manager 6.0.

Note Before performing the migration, verify that the user names configured for Cisco Unified Mobility are also configured in Cisco Unified Communications Manager. Specifically, if *user1* is the Cisco Unified Mobility user whose data will be migrated to Cisco Unified Communications Manager, *user1* must already be in the Cisco Unified Communications Manager database.

Note Cisco Unified Communications Manager 6.0 does not allow remote destination numbers to be shared; therefore, you must remove any duplication during migration.

Note The remote destination number in Cisco Unified Mobility may have a 9 or 91 prefix access code. Confirm that these prefixes are consistent with the Cisco Unified Communications Manager 6.0 configuration during migration.

Migration Files

The data files listed in this section must be migrated to Cisco Unified Communications Manager.

CMMRDProfile.csv

This file contains the following fields:

REMOTE DESTINATION PROFILE NAME,DESCRIPTION,USER ID,DIRECTORY NUMBER 1,CSS,DEVICE POOL

REMOTE DESTINATION PROFILE NAME is taken from the Mobile Voice Access User ID field in Cisco Unified Mobility. CSS and DEVICE POOL are derived from an AXL query from Cisco Unified Communications Manager

In the DESCRIPTION field, the tool adds a default description, *userID*_RDP.

Example:

1681000RDP,johndoe_RDP,johndoe,1681000,everyonecss,Default

CMMAccessList.csv

This file contains the following fields:

ACCESS LIST NAME,ACCESS LIST DESCRIPTION,ACCESS LIST ALLOWED,ACCESS LIST OWNER,ACCESS LIST MEMBER 1

Example:

allow1,,t,johndoe,5551212

CMMRemoteDestination.csv

This file contains the following fields:

DESTINATION,NAME,DUAL MODE DEVICE,REMOTE DESTINATION PROFILE,ISMOBILEPHONE,ANSWER TOO SOON TIMER,ANSWER TOO LATE TIMER,DELAY BEFORE RINGING TIMER,ACCESS LIST ALLOWED,ACCESS LIST BLOCKED,SMART CLIENT INSTALLED,ENABLE MOBILE CONNECT,ASSOCIATED LINE NUMBER,PARTITION

In the DESTINATION NAME field, the tool adds a default name *userID*_RD.

Example:

95551212,johndoe_RD,f,1681000,t,1500,0,0,,,f,t,1681000,

CMMUserEnable.csv

This file contains the following fields:

USER ID,ENABLE MOBILITY,ENABLE MOBILE VOICE ACCESS

Example:

johndoe,t,t

CMMFeatureDataExport.log

This log contains warning messages.

Example:

```
Feature Data checking starts -----.
Remote Destination 95551212 has been associated with two users: 1681000RDP and 1682000RDP.
Feature Data checking ends -----.
```

Follow this process to migrate standalone Cisco Unified Mobility data to Cisco Unified Communications Manager Release 6.0(1):

Procedure

Step 1 Log into Cisco Unified Mobility and export the configuration data files in CSV format:

- Use **Export** > **Feature Data** for CMMRDProfile.csv, CMMAccessList.csv, CMMRemoteDestination.csv, and CMMUserEnable.csv.
- Use **Export** > **Log** for CMMFeatureDataExport.log.

Step 2 Log into Cisco Unified Communications Manager Administration Release 6.0(1). Choose **Bulk Administration** > **Upload/Download Files** to upload the four CSV files.

Step 3 Choose **Bulk Administration> Mobility > Remote Destination Profile> Remote Destination Profile Template** to create a template and its associated line template. In the Rerouting Calling Search Space field, enter the value taken from the Outgoing CTI port Calling Search Space in your old Cisco Unified Communications Manager system.

Step 4 Choose **Bulk Administration > Mobility > Remote Destination Profile**, and insert the file CMMRDProfile.csv. Check the error log to verify that no error occurs.

Step 5 Choose **Bulk Administration > Mobility > Access List**, and insert the file CMMAccessList.csv. Check the error log to verify that no error occurs.

Step 6 Choose **Bulk Administration > Mobility > Remote Destination**, and insert the file CMMRemoteDestination.csv. Check the error log to verify that no error occurs.

Step 7 Choose **Bulk Administration > Users**, and update the file CMMUserEnable.csv. Check the error log to verify that no error occurs.

Multilevel Precedence and Preemption (MLPP) Supplementary Services

Introduced in Cisco Unified Communications Manager Release 4.2(3), MLPP Supplementary Services support the following features:

- MLPP Support for Multiple Appearance Lines—The system currently supports MLPP support for multiple appearance lines.
- Call Forwarding—Ensure no precedence calls are forwarded to off-net endpoints (for example, cell phones). Additionally, ensure forwarded calls retain the original precedence across multiple forwarding hops.
  - For CFA (Call Forward All) scenarios, precedence calls will get routed to the AP target of the original called party immediately. The CFA target does not get used for MLPP calls.
  - For CFB (Call Forward Busy) scenarios, precedence calls will get forwarded to the configured CFB destination, subject to the hop count limits that were previously described and the state of open appearances on the called party endpoint.
  - For the CFNA (Call Forward No Answer) scenario, the system attempts a single forward attempt (hop) to the CFNA target of the original called party. If that endpoint does not answer prior to the no answer timer expiring, the call then gets sent to the MAP target of the original called party.
- Three-Way Calling—The three-way calling enhancement allows each connection of a three-way call to maintain its original precedence level. The phone that is performing the split operation of the three-way call uses the higher precedence level of the two calls when different precedence levels are used. This enhancement also supports preemption of conference bridge resources. If a conference bridge is saturated with calls, individual streams gets preempted when a new, higher precedence, three-way call gets set up.
- Transfer—When a call transfer is made at different precedence levels, the switch that initiates the transfer class marks the connection at the highest precedence level of the two segments.

This enhancement upgrades the precedence level of a call leg that is involved in a transfer operation. For example, party A calls party B at Priority. Party B then initiates a transfer to C and dials the Flash precedence digits when dialing. When the transfer completes, the precedence level of party A gets upgraded from Priority to Flash.

Note The precedence level upgrade does not work over ICT or PRI trunks.

- Call Pickup—This enhancement adds the criteria of highest precedence to the call pickup algorithm. The enhancement includes the following requirements:
  - If a call pickup group has more than one party in an unanswered condition, and the unanswered parties are at different precedence levels, a call pickup attempt in that group will retrieve the highest precedence call first.
  - If multiple calls of equal precedence are ringing simultaneously, a call pickup attempt in that group will retrieve the longest ringing call first.
  - This release supports group pickup functionality for MLPP calls. Operation follows normal call pickup functionality.
  - For MLPP calls, this release does not support Other Group Pickup.
- Hunt Pilot/Hunt List—Normal hunt algorithm logic occurs until all lines in the hunt group are busy. When all lines are busy, the lowest precedence call gets selected for preemption. When preemption occurs, normal line group 'no answer' timer continues. When timer expires, next lowest precedence call in hunt group gets selected for preemption. MLPP enhancements support the following three hunt algorithms:
  - Top down
  - Longest idle time
  - Circular

Cisco Unified Communications Manager allows multiple line groups to be configured for a hunt group.

Where to Find More Information

- *Cisco Unified IP Phone User Guides*
- MultiLevel Presence and Preemption, *Cisco Unified Communications Manager Features and Services Guide*
- Service Activation, *Cisco Unified Serviceability Administration Guide*
- *Release Notes for Cisco Unified Communications Manager Release 4.2(3)*

Multilevel Precedence and Preemption Enhancements

Introduced in Cisco Unified Communications Manager Release 4.2(1), MLPP includes the following additional features for the Defense Red Switched Network (DRSN):

- Support to map MLPP precedence levels to DSCP values in the TOS field of the IP header
- Support for MLPP-enabled, UUIE-based PRI-4ESS interface across intercluster trunks
- V150.1 Modem Relay support for Cisco Unified Communications Manager intercluster trunking configurations

Introduced in Cisco Unified Communications Manager Release 4.2(1), the following configuration enhancements to MLPP support these features:

- UUIE Configuration on H.225 and Intercluster Trunk Configuration window for 4ESS protocol:
  - Passing Precedence Level Through UUIE
  - Security Access Level

- You can map the following precedence levels to DSCP values in the Service Parameters window:
  - Executive Override
  - Flash Override
  - Flash
  - Immediate
  - Priority

Tunneling of MLPP precedence level information can get carried in a PRI UUIE across an H.323 intercluster trunk via nonstandard control data within a H.225 UUIE.

DSCP marking creates multiple expedited forwarding classification levels that correspond to MLPP precedence levels.

Where to Find More Information

- Introducing MLPP, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*

Recording and Monitoring

Cisco Unified Communications Manager supports silent call monitoring and call recording. Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The Silent Call Monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session. (Other call monitoring modes include whisper call monitoring and active call monitoring, which the current release of Cisco Unified Communications Manager does not support.)

The Call Recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.

Cisco Unified Communications Manager Administration Configuration Tips

Perform the following steps to configure monitoring and recording:

1. Turn on IP phone built-in bridge (BIB) to allow monitoring or recording.
2. Add user for monitoring or recording application.
3. Add user to groups that allow monitoring and recording.
4. Configure tones for monitoring or recording.
5. Configure DN for monitoring calling search space.
6. Enable recording for a line appearance.
7. Create recording profile.
8. Create a SIP trunk that points to the recorder.
9. Create a route pattern for the recorder.
10. Create recorder redundancy.

Refer to the Monitoring and Recording chapter of the *Cisco Unified Communications Manager Features and Services Guide* for configuration details.

GUI Changes

The following new and changed windows support recording and monitoring:

- Recording Profile Configuration (**Device > Device Settings > Recording Profile**)

Service Parameter Changes

The following new service parameters support recording and monitoring:

- Play Recording Notification Tone To Observed Target
- Play Recording Notification Tone To Observed Connected Parties
- Play Monitoring Notification Tone To Observed Target
- Play Monitoring Notification Tone To Observed Connected Parties
- G722 Codec Enabled
- iLBC Codec Enabled
- Built-in Bridge Enable

CTI Considerations

Computer Telephony Integration (CTI), Java Telephony API (JTAPI), and TSP support monitoring and recording of calls. Applications can use these interfaces to monitor or record calls in a Cisco Unified Communications Manager system. CTI provides the ability for applications to monitor calls on a per-call basis.

Call reference for the recorded call (agent-customer call) gets passed to the recorder. The recording application needs to get other relevant information through the CTI interface.

When invoking recording and monitoring or any other CTI features, delays and unexpected behavior can result if UDP transport is used for SIP phones.

Security Considerations

To meet with the security requirements, the system allows call monitoring and call recording only when the monitoring calls or the recording calls can be established with the same or higher security levels as the security level of the call that is monitored or recorded. When such conditions cannot be met, the monitoring request or the recording request gets rejected with appropriate cause codes.

To implement the behavior in Cisco Unified Communications Manager that the security requirements for monitoring and recording dictate, the system uses a phased approach. In the first phase, the system permits monitoring or recording sessions only for an IP phone that does not have security enabled. When an application requests monitoring and recording sessions for a security-enabled phone, the request gets rejected with an appropriate cause code.

BAT Considerations

The monitoring and recording features interact with the Bulk Administration Tool (BAT).

Where to Find More Information

- Monitoring and Recording, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Application User Configuration, *Cisco Unified Communications Manager Administration Guide*
- User Group Configuration, *Cisco Unified Communications Manager Administration Guide*
- Service Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*

- Directory Number Configuration, *Cisco Unified Communications Manager Administration Guide*
- Recording Profile Configuration, *Cisco Unified Communications Manager Administration Guide*
- Route Pattern Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*

Cisco Unified Communications Manager Bulk Administration Features

Cisco Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, performs bulk transactions to the Cisco Unified Communications Manager database. This section introduces the changes to BAT for Cisco Unified Communications Manager 6.0.

New and Changed Information for BAT

The following changes in BAT apply for Cisco Unified Communications Manager Release 6.0:

- Adding and Updating Intercom DNs—You can use BAT to add and update intercom directory numbers in bulk. You access this feature from **Bulk Administration > Phones > Add/Update Intercom**.
- Updating and Exporting Line Appearances—You can use BAT to export and update information about line appearances. You access this feature from **Bulk Administration > Users > Line Appearance**.
- Inserting VG224 Gateways—You can use BAT to insert VG224 gateways in bulk. You can do this through **Bulk Administration > Gateways > Insert Gateways**.
- Creating and Adding Gateway File Formats—You can use BAT to configure gateway file formats. You access this feature from **Bulk Administration > Gateways > Gateway File Format**.
- Working with Mobility:
  - Access Lists—You can use the Bulk Administration menu to insert, delete, and export access lists. You access this feature from **Bulk Administration > Access List**.
  - Working with Remote Destinations—You can use BAT to insert, delete, and export remote destination details in bulk. Access this feature from **Bulk Administration > Mobility > Remote Destination**.
  - Working with Remote Destination Profiles—You can use BAT to format, insert, delete, and export Remote Destination Profiles (RDPs) in batches. You access this feature from **Bulk Administration > Mobility > Remote Destination Profile**.
- Importing/Exporting Configuration—You can use the Import/Export menu in BAT to export or import all or a part of the Cisco Unified Communications Manager database to another server, or to the same server with modifications. You access this feature from **Bulk Administration > Import/Export**.

BAT Configuration Tips

Access all BAT configuration from the Cisco Unified Communications Manager Administration menu.

GUI Changes

Cisco Unified Communications Manager Administration includes a menu item called Bulk Administration. The following changes occurred in the GUI for BAT in Cisco Unified Communications Manager 6.0:

- **Bulk Administration > Phones > Add/Update Intercom**
  - Update Intercom DNs
  - Add Intercom DNs
- **Bulk Administration > Users > Line Appearance**
  - Export Line Appearance
  - Update Line Appearance
- **Bulk Administration > Gateways > Gateway File Format**
  - Create File Format
  - Add File Format
- **Bulk Administration > Import Export**
  - Export
  - Import
- **Bulk Administration > Mobility**
  - Access List
  - Remote Destination
  - Remote Destination Profile

Where to Find More Information

- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Communications Manager Security Features

Cisco Unified Communications Manager 6.0 supports the following security features:

- Secure Conferencing, page 71
- Secure Conference Icon, page 74

Secure Conferencing

The Secure Conferencing feature provides authentication and encryption to secure a conference. Consider a conference as secure when all participating devices have encrypted signaling and media. The secure conference feature supports SRTP encryption over a secure TLS or IPSec connection.

The system provides a security icon for the entire conference, which is determined by the lowest security level of the participating devices. For example, a secure conference that includes two encrypted connections and one authenticated connection represents a conference security status of authenticated.

Conference status can change as participants enter and leave the conference. An encrypted conference session can revert to a security level of authenticated or nonsecure if an authenticated or nonsecure participant connects to the call. Likewise, the session status can upgrade if an authenticated or nonsecure participant drops off the call. A nonsecure participant that connects to a conference call renders the conference session nonsecure.

As administrator, you can specify a minimum security level for a conference when you configure a Meet-Me pattern or number as authenticated or encrypted. Participants must meet the minimum security requirement, or the system blocks the participant and drops the call.

To secure conferences with barge, configure phones to use encrypted mode. After the Barge key is pressed and if the device is authenticated or encrypted, Cisco Unified Communications Manager establishes a secure connection between the barging party and the built-in bridge at the target device. The system provides a conference security status for all connected parties in the barge call. See the "Barge Enhancements" section on page 29 for secure conference considerations with barge.

Warning **To obtain the full benefit of secure conference features, Cisco recommends upgrading Cisco Unified IP Phones to firmware release 8.3, which supports the encryption features in this release. Encrypted phones that run earlier releases do not fully support these new features. These phones can only participate in a secure conference as authenticated or nonsecure participants.**

Cisco Unified IP Phones that are running firmware release 8.3 with an earlier release of Cisco Unified Communications Manager will display their connection security status during a conference call, not the conference security status, and do not support secure conference features like conference list.

Cisco Unified Communications Manager supports secure conference over licensed CTI devices.

Cisco Unified Communications Manager supports secure conference over intracluster trunks (ICTs), H.323 trunks/gateways, and MGCP gateways; however, encrypted phones that are running firmware release 8.2 or earlier will revert to RTP for ICT and H.323 calls, and the media is not encrypted.

If a conference involves a SIP trunk, the secure conference status specifies nonsecure. In addition, SIP trunk signaling does not support secure conference notifications to off-cluster participants.

Cisco Unified Communications Manager Administration Configuration Tips

A conference bridge can register as a secure media resource when you add a hardware conference bridge to your network and you configure a secure conference bridge in Cisco Unified Communications Manager Administration.

Consider the following information before you configure secure conference bridge resources:

- Use localization if you want the phone to display custom text for secure conference messages. Refer to the *Cisco Unified Communications Operating System Administration Guide* for information about the Locale Installer.
- The conference or built-in bridge must support encryption to secure conference calls.
- To enable secure conference bridge registration, set the cluster security mode to mixed mode.
- Ensure the phone that initiates a conference is authenticated or encrypted to procure a secure conference bridge.
- To maintain conference integrity on shared lines, do not configure devices that share a line with different security modes; for example, do not configure an encrypted phone to share a line with an authenticated or nonsecure phone.
- Do not use SIP trunks as ICTs when you want to share conference security status between clusters.

- If you set the cluster security mode to mixed mode, the security mode that is configured for the DSP farm (nonsecure or encrypted) must match the conference bridge security mode in Cisco Unified Communications Manager Administration, or the conference bridge cannot register. The conference bridge registers as encrypted when both security modes specify encrypted; the conference bridge registers as nonsecure when both security modes specify nonsecure.
- If you set the cluster security mode to mixed mode, if the security profile that you applied to the conference bridge is encrypted, but the conference bridge security level is nonsecure, Cisco Unified Communications Manager rejects conference bridge registration.
- If you set the cluster security mode to nonsecure mode, configure the security mode at the DSP farm as nonsecure, so the conference bridge can register. The conference bridge registers as nonsecure even if the setting in Cisco Unified Communications Manager Administration specifies encrypted.
- During registration, the conference bridge must pass authentication. To pass authentication, the DSP farm must contain the Cisco Unified Communications Manager certificate, and Cisco Unified Communications Manager must contain certificates for the DSP farm system and the DSP connection. To ensure the conference bridge passes authentication, the X509 certification name must contain the conference bridge name.
- If conference bridge certificates expire or change for any reason, use the certificate management feature in the Cisco Unified Communications Operating System Administration to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and conference bridge does not work because it cannot register to Cisco Unified Communications Manager.
- The secure conference bridge registers to Cisco Unified Communications Manager through TLS connection at port 2443; a nonsecure conference bridge registers to Cisco Unified Communications Manager through TCP connection at port 2000.
- Changing the device security mode for the conference bridge requires a reset of Cisco Unified Communications Manager devices and a restart of the Cisco CallManager service.
- To configure packet capturing for a secure conference bridge, enable packet capturing in the Service Parameter Configuration window; then, set the packet capture mode to batch mode and capture tier to SRTP for the phone, gateway, or trunk in the device configuration window.

GUI Changes

The following new and changed windows in Cisco Unified Communications Manager Administration contain secure conferencing configuration settings:

- **Media Resources > Conference Bridge Configuration**
  - Device Security Mode

Note You must select Cisco IOS Enhanced Conference Bridge as the conference bridge type.

- **Call Routing > Meet-Me Number/Pattern**
  - Minimum Security Level

Removed or Changed Service or Enterprise Parameters

To keep a conference secure, if a participant in a secure ad hoc conference puts a call on hold or parks the call, the system does not play MOH, even if the Suppress MOH to Conference Bridge service parameter is set to False. The secure conference status does not change.

Serviceability Considerations

CDR data provides the security status of each call leg from the phone endpoint to the conference bridge as well as the security status of the conference itself. The two values use two different fields inside the CDR database.

CDR data provides termination cause code 58 (Bearer capability not presently available) when a Meet-Me conference rejects a join attempt that does not meet the minimum security level requirement.

This features includes no new performance objects, counters, or alarms.

User Tips

When users with secure phones initiate standard (ad hoc) conference calls or meet me conference calls, Cisco Unified Communications Manager assigns a secure conference bridge. An icon (lock or shield) displays next to "Conference" on the phone window to indicate the security level of the conference. If a participant with a nonsecure phone joins the conference, the icon changes to a "call in progress" icon to indicate that the conference is no longer secure.

Non-secure participants and non-secure conferences show the call state icon for "connected call."

Where to Find More Information

- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Troubleshooting Guide*

Secure Conference Icon

Cisco Unified IP Phones display a conference security icon for the security level of the entire conference. These icons match the status icons for a secure, two-party call, as described in the user documentation for your phone.

For ad hoc and meet-me secure conferences, the security icon for the conference session displays next to the conference softkey in the phone screen for conference participants. The icon that displays depends on the security level of the conference bridge and all participants.

A conference list displays on participating phones when the ConfList softkey is pressed during a conference call. The conference list provides the conference status as well as the security status for each participant to identify participants that are not encrypted. Conference list displays these security icons: nonsecure, authenticated, encrypted, held. The conference initiator can use the conference list to eject participants with a low security status.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether conference participants other than the conference initiator can eject conference participants.

When a user presses Barge, the icon that displays next to the Barge softkey provides the security level for the barge conference. If the barging device and the barged device support encryption, the system encrypts the media between the two devices, but the barge conference status can be nonsecure, authenticated, or encrypted, depending on the security levels of the connected parties. See the "Barge Enhancements" section on page 29 for secure conference icon considerations with barge.

During a packet capture session, the phone displays a nonsecure status for the conference, even if the media stream is encrypted.

Cisco Unified Communications Manager Administration Configuration Tips

Secure conference icons display when you configure a secure conference bridge in Cisco Unified Communications Manager Administration or barge secure phones.

Removed or Changed Service or Enterprise Parameters

If a participant in a secure ad hoc conference puts a call on hold or parks the call, the system does not play MOH, even if the Suppress MOH to Conference Bridge service parameter is set to False, to keep the conference secure. The secure conference status does not change.

Where to Find More Information

- *Secure Conferencing, page 71*
- *Cisco Unified Communications Manager Security Guide*

Cisco Unified Serviceability

Cisco Unified Communications Manager Release 6.0(1) provides the following enhancements to Serviceability:

Tip In previous releases of Cisco Unified Communications Manager, the DBReplicationFailure alert was generated based on the DBReplicationFailure alarm. In Cisco Unified Communications Manager 6.0(1), the DBReplicationFailure alert gets generated when the value for the Replication_State performance monitoring counter specifies 1, 3, or 4. No alert gets generated if the value specifies 0 or 2. For more information see the "Number of Replicates Created and State of Replication" section on page 140.

Serviceability Administration

Cisco Unified Serviceability allows you to perform such tasks as configuring trace parameters, configuring alarms, and activating, starting, and stopping services for Cisco Unified Communications Manager.

GUI Changes

The Cisco Unified Serviceability GUI contains the following changes for this release:

- Serviceability Administration name change—The serviceability administration GUI name changed from Cisco Unified CallManager Serviceability to Cisco Unified Serviceability.
- System Alarm Catalog (new)—The System Alarm Catalog, which displays in the Alarms Messages Definition window (**Alarms** > **Definitions**), contains the following alarm catalogs: ClusterManagerAlarmCatalog, DBAlarmCatalog, DRFAlarmCatalog, GenericAlarmCatalog, JavaApplications, LoginAlarmCatalog, LpmTctCatalog, RTMTAlarmCatalog, SystemAccessCatalog, ServiceManagerAlarmCatalogs, TFTPAlarmCatalog, and TestAlarmCatalog.

The MLAAlarmCatalog, which was introduced in release 4.2(3), no longer exists in Cisco Unified Serviceability. The LoginAlarmCatalog (new) replaces the MLAAlarmCatalog, and the AuthenticationFailedAuthenticationFailed alarm replaces the MLAUserLoginFailed alarm. The LoginAlarmCatalog contains all login-related alarm definitions, including the AuthenticationFailed alarm. For information on this alarm, search for the alarm (**Alarms > Definitions**) and click the alarm name after it displays. In addition, the clusterwide precanned alert, AuthenticationFailed, now replaces MLAUserLoginFailed. AuthenticationFailed gets triggered when the alarm threshold is met, so the system sends an e-mail or page.

The ClusterManagerAlarmCatalog (new) contains all cluster manager alarm definitions that are related to the establishment of security associations between nodes in a cluster. The Service Manager Alarm Catalogs contains all service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services. The SystemAccess Catalog (new) contains all alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters. The *Cisco Unified Serviceability Administration Guide* describes all other preceding catalogs, which existed in previous releases.

CallManager Alarm Catalog (changed)—The CallManager Alarm Catalog, which displays in the Alarms Messages Definition window (**Alarms > Definitions**), contains the following alarm catalogs: CDRRepAlarm Catalog, CEFAlarmCatalog, CMIAlarmCatalog, CtiManagerAlarmCatalog, IpVmsAlarmCatalog, and TCDSRVAlarm Catalog. The *Cisco Unified Serviceability Administration Guide* describes all preceding catalogs, which existed in previous releases.

- Services Group drop-down list box (new)—This setting displays in the Alarm Configuration and Trace Configuration windows (**Alarm > Configuration and Trace > Configuration**). Cisco Unified Serviceability categorizes services into groups. Before you can configure a trace or alarm for a service, you must choose the service group for the service that you want to configure for trace or alarms. After you choose the service group, you can choose the service from the Service drop-down list box.

  Refer to the "Configuring Alarms" and "Configuring Trace" chapters in the *Cisco Unified Serviceability Administration Guide* for a list of services that correspond to the service groups that are used in alarm and trace configuration.

- In the Control Center—Feature Services and Control Center—Network Services windows (**Tools > Control Center...**), the Start Time (new) and Up Time (new) columns display. The Start Column displays when the services was last started, and the Up Time column displays the time that the service has been running.

- Check All Services check box (new)—If you want to activate all services that display in the Service Activation window (**Tools > Service Activation**), check this check box.

Administration Configuration Tips

- In Cisco Unified Communications Manager 6.0(1), you can log directly in to Cisco Unified Serviceability (without first logging in to Cisco Unified Communications Manager Administration). In Netscape 7.1 or Internet Explorer 6.0, enter **https://<server name or IP address>:8443/ccmservice/**, where server name or IP address equals the server where the Cisco Unified Serviceability service runs, and 8443 equals the port number for HTTPS.

  After you log in to Cisco Unified Serviceability, you can access all applications that display in the Navigation drop-down list box, except for the Cisco Unified Communications Operating System Administration or Disaster Recovery System, without having to log in to each application. You cannot access the Cisco Unified Communications Operating System or Disaster Recovery System GUIs with the same password that you use to log in to Cisco Unified Serviceability. To access these

applications from Cisco Unified Serviceability, you must click the **Logout** link in the upper, right corner of the Cisco Unified Serviceability window; then, choose the application from the Navigation drop-down list box and click **Go**.

If you have already logged in to one of the applications that display in the Navigation drop-down list box (not Cisco Unified Communications Operating System Administration or Disaster Recovery System), you can access Cisco Unified Serviceability without logging in; from the Navigation drop-down list box, choose Cisco Unified Serviceability; then, click **Go**.

- In previous releases, two guides supported Cisco Unified Communications Manager Serviceability: the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*. In Cisco Unified Communications Manager 6.0(1), refer to the *Cisco Unified Serviceability Administration Guide* for descriptive and procedural information on how to configure Cisco Unified Serviceability.

  The *Cisco Unified Serviceability Administration Guide* does not contain detailed information on the Real-Time Monitoring Tool (RTMT). For information on how to use RTMT, refer to the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

Service Enhancements

Cisco Unified Communications Manager Release 6.0(1) includes the following enhancements for services:

- The Cisco Unified Voice Access Service, a new feature service that exists under the CM Service group, starts the mobile voice access capability within Cisco Unified Mobility; mobile voice access, which is an integrated voice response (IVR) system, allows Cisco Unified Mobility users to perform the following tasks:
  - Make calls from the cellular phone as if the call originated from the desk phone.
  - Turn Cisco Unified Mobility on; turn Cisco Unified Mobility off.

  For mobile voice access to work, you must activate the service, which you do on one server in the cluster after you configure the H.323 gateway to point to the first VXML page. In addition, make sure that the Cisco CallManager and the Cisco TFTP services run on one server in the cluster, not necessarily the same server where the Cisco Unified Voice Access Service runs.
- In the Control Center—Feature Services and Control Center—Network Services windows, the Start Time and Up Time columns display.
- Cisco Unified Serviceability displays the Service Groups drop-down list box, which is described in the "GUI Changes" section on page 75.
- For information on stopping and starting some services through the command line interface (CLI), refer to the *Cisco Unified Communications Operating System Administration Guide*.

New Service Parameters

This parameter specifies the maximum number of Processes and Threads that is allowed for SystemAccess to provide the complete Process and Thread statistics counters. If the total number of Processes/Threads exceeds this maximum number, SystemAccess only provides up to the maximum number of Processes statistics counters and ccm Thread (if running) statistics counters. The system provides no other Thread statistics counters.

To configure the maximum number of processes and threads, access the Maximum Number of Process and Threads service parameter for the Cisco RIS Data Collector service in Cisco Unified Communications Manager Administration. Click the hyperlink for the parameter name to display the question mark help, which contains more information on the parameter, including the default value.

AXL Considerations

For information on the AXL Serviceability API, refer to the *Cisco Unified Communications Manager Developers Guide for Release 6.0*.

Where to Find More Information

- *Cisco Unified Serviceability Administration Guide*
- Service Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Developers Guide for Release 6.0*
- *Cisco Unified Communications Operating System Administration Guide*

Cisco Unified Real-Time Monitoring Tool

Cisco Unified Communications Manager 6.0 includes the following changes to the Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT):

- Trace and Log Central added an option that allows you to collect installation and upgrade log files on your local computer.
- The new LogFileSearchStringFound alert replaces the TraceCollectionToolEvent alert. If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert.
- The new CpuPegging alert replaces the NonCallProcessingNodeCpuPegging alert. The existing threshold setting for NonCallProcessingNodeCpuPegging does not get preserved, but the default CPU threshold settings for CpuPegging will remain the same as the NonCallProcessingNodeCpuPegging alert.
- RTMT added the following performance objects:
  - Cisco MGCP BRI Device—The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object includes performance counters with information about registered Cisco MGCP BRI devices.
  - Cisco MobilityManager—The Cisco Mobility Manager object includes performance counters with information on registered Cisco Unified Mobility Manager devices.
  - Cisco SIP Station—The Cisco SIP Station object includes performance counters with information about registered Cisco SIP Stations.
  - Cisco Signaling Performance—The Cisco Signaling Performance object provides call signaling data on transport communications on Cisco Unified Communications Manager.
- RTMT added the following performance counters (object):
  - SIPTrunkAuthorizationFailures (Cisco CallManager)
  - SIPTrunkAuthorizations (Cisco CallManager)
  - CallsRejectedDueToICTCallThrottling (Cisco H.323)
  - CCBsAllocated (Cisco SIP Stack)
  - PublishIns (Cisco SIP Stack)
  - PublishOuts (Cisco SIP Stack)
  - SCBsAllocated (Cisco SIP Stack)
  - SIPHandlerSDLQueueSignalsPresent (Cisco SIP Stack)
  - SIPGenericCounter1 through SIPGenericCounter4 (Cisco SIP Stack)

GUI Changes

- The name of the Cisco Unified CallManager Real-Time Monitoring Tool changed to Cisco Unified Communications Manager Real-Time Monitoring Tool.
- The reorganized user interface for Cisco Unified Communications Manager Real-Time Monitoring Tool represents a directory tree under different tabs based on whether you are interested in monitoring the system and server object or whether you are monitoring objects that are related to Cisco Unified Communications Manager. You can access the following tabs by clicking on the quick launch channel on the left pane of the RTMT window.
  - The System tab includes tools that help you monitor predefined system objects—System Summary, CPU and Memory Usage, Process, Disk Usage, Critical Services, Performance, Performance Log Viewer, Alert Central, Trace & Log Central (formerly known as Trace Collection Tools), and SysLog Viewer.
  - The CallManager tab includes tools that help you monitor predefined Cisco Unified Communications Manager objects—Communications Manager Summary, Call Activity, Gateway Activity, Trunk Activity, SDL Queue, SIP Activity, Device summary, Device Search, Phone Summary, Cisco TFTP, Heartbeat, Database, Summary, CTI Manager, CTI search.
  - RTMT adds icons to the directory trees for plug-ins, such as Voice Log Translator (VLT) application, that get installed on RTMT.
- Critical Services now comprise groups based on whether the service is a System service or Cisco Unified Communications Manager (CallManager) service. RTMT displays the status of each service in the window when you click the appropriate tab.
- Alerts now comprise groups based on whether the alert is a System alert, a Cisco Unified Communications Manager (CallManager) alert, or a user-defined alert. RTMT displays alert status in the window when you click the appropriate tab. User-defined alerts represents custom alerts.
- The System Summary window now includes an alert history table.

Administration Configuration Tips

- When you collect or view a trace file or dump file for a particular service in Trace and Log Central, you will find that the services are grouped based on whether the service is a system service or a Cisco CallManager service.
- When you select a trace file for viewing by using the Remote Browse feature in Trace and Log Central, you can now choose the RTMT, and you can choose the type of viewer that you would like to use to display the file.
- The local Browse feature in Trace and Log Central allows you to choose one of the Cisco-provided viewers, like the Cisco Generic Viewer or another program, as the default viewer of your choice for viewing the log files with that file extension.

Where to Find More Information

- *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

Cisco Unified Communications Manager CDR Analysis and Reporting

The Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) application generates reports for calls on the basis of call detail records (CDRs) and call management records (CMRs). For this release, the following changes apply to CAR:

- When a logged-in Cisco Extension Mobility user makes a call, CAR uses the user ID that is configured for the Cisco Extension Mobility user in all reports that display a user ID. When the call is made by a non-Cisco Extension Mobility user (or logged-out Cisco Extension Mobility user) and when the call is made with a device that does not have a configured Owner User ID, CAR uses the default user ID, unspecifieduser, in the report.
- CDR Search includes several changes:
  - Mobility and Silent Monitoring and Recording calls comprise additions as new call features. The resulting CDR Search report window will show the new call types listed in the CallType column.
  - The origConversationID and callSecuredStatus fields display in the CDR detail reports.
- A Busy Hour Call Completion (BHCC) number with the percentage of traffic during the busy hour now displays in the header of the Traffic Summary (hour of day) report.
- Application users that have been added to the Standard CAR Administration group as a CAR Administrator can log in to CAR as an administrator with access to all CAR reports except the Individual Bill Report. If non-CAR Administrator application users try to log in, the following message displays: “Either the User Name or the Password entered is invalid. Ensure that you are logging into CAR as a CAR administrator or a regular End User.”
- The CAR Loader feature redesign for Cisco Unified Communications Manager Release 6.0(1) improves the overall CAR loader performance. The loading rate of CDRs and CMRs into the CAR database improved. A new option exists to load only CDRs into the CAR database and not load the CMRs. The CAR Loader will now load all CDRs into the CAR database first, and those CDRs will get updated with the CMR information after all CDRs within the same date are loaded into the database. Also, a new Unfinished-Processing-File-Recovery capability allows the CAR Loader to recover loading unfinished-processing CDR/CMR flat files properly.
- When administrators configure phones from Cisco Unified Communications Manager Administration and do not specify the Owner User ID, the CAR Loader cannot determine the user_id that is associated with the device during load. For all these calls, CAR will assign the value of “unspecifieduser” to the user_id column of the CAR database. When you run a report, you will see a user that is called _unspecifieduser in the CAR reports.
- CAR now supports the new error codes that the Identity Management System (IMS) returns and the corresponding error messages. The user sees the appropriate error message on the CAR Invalid Logon window.
- New CAR report algorithms that have been implemented reduce the user-selected date and time range, so the number of records in the newly narrowed date and time range fall between 5000 and 10,000 records for PDF reports, between 20,000 and 30,000 records for CSV reports, and between 100 and 200 records for CDR Search reports. The narrowed date and time range that get returned from the algorithm provides the basis for report generation, and not the user-selected date and time range that users input.
- Under Device Reports, changes reduce the number of gateways that can be searched in the Gateway Utilization Report from 15 to 5. The manner of calculating the gateway utilization also changed. Gateway utilization now gets calculated based on the duration of calls instead of the number of calls.
- The method for configuring the H.323 Gateway Utilization report has been changed. No port information for H.323 gateways is stored in the Cisco Unified Communications Manager database. The H.323 gateway port information must be obtained from the Gateway Configuration window in CAR. Choose **System > System Parameters > Gateway Configuration** to configure the H.323 gateway ports.

- This change applies mainly to H.323 gateways and to any other gateways that have no port information available in the Cisco Unified Communications Manager database. Port information is available in the Cisco Unified Communications Manager database for most of the other types of gateways.
- When the Forced Authorization Code (FAC) feature is invoked, the authorizationCodeValue field is written into the CDR. To display the authorizationCodeValue field information in the CDR, the "Display FAC in CDR" service parameter must be set to True. The default value of the parameter is False.

GUI Changes

The CAR GUI contains the following changes for this release:

- The CDR Search changed to select the date and time in Coordinated Universal Time (UTC) format (date and time in which the files were generated on the server) as opposed to prior releases that were based on local date and time.
- The CDR Search window adds Mobility and Silent Monitoring and Recording to the CallType column.
- The CAR Loader changed to add Mobility and Silent Monitoring and Recording to the call types.
- When the CAR administrator configures the CAR Loader through **System** > **Scheduler** > **CDR Load**, the administrator can use two new options that are available. The first option, Load CDR Only, allows the administrator to choose not to load the CMRs into the CAR database. The second option, Continuous Loading 24/7, allows the administrator to immediately start the CAR Loader and let it run continuously 24 hours a day, 7 days a week, to load CDR/CMR records in near real-time fashion.
- The Gateway Utilization Report found in the Device Reports changes the maximum number of gateways, route groups/line groups, route lists/hunt lists, route patterns/hunt pilots, and voice mail ports from 15 to 5.

Administration Configuration Tips

Use the following tips to configure and use CAR:

- When you configure the time range for CDR Search, use UTC. Likewise, when you configure the date and time range settings for CDR Search, configure the settings, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays that you must revise the settings.

Where to Find More Information

- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Cisco Unified Serviceability Administration Guide*

Call Detail Record Definitions

This section describes the changes to the CDRs and CMRs with this release.

- With Cisco Unified CallManager Release 4.2(1), you can configure Cisco Unified CallManager to report the directory number (DN) of the hunt group member who answered a direct call to the hunt pilot number in the final called party number field in the CDR. Previously, Cisco Unified CallManager reported the hunt pilot DN in the final called party number field in the CDR.

- Cisco Unified CallManager Release 4.2(3) provides advanced ad hoc conference enhancements including the addition of the origConversationID field to the CDR.This field identifies the conference ID that is associated with the originating leg of the call. In most cases, this field equals 0. Default equals 0. The destConversationID field was added in previous releases. For conference chaining scenarios, the origConversationID and destConversationID fields identify which conferences are chained together.

  The requestor party (party that requested the removal of a participant) appears in the CDR comment field to track the drop requestor because the requestor can be a participant other than the controller. The following tags apply for the originator information: ConfRequestorDn and ConfRequestorDeviceName. The tags for the drop requestor information include DropConfRequestorDn and DropConfRequestorDeviceName.

- Cisco Unified Communications Manager Release 6.0(1) eliminates CDR Configuration Enterprise Parameters that were available in previous releases. To locate the CDR Configuration Enterprise Parameters, open Cisco Unified CallManager Administration and choose **System** > **Enterprise Parameters**. The release eliminates the following parameters:
  - Local CDR Path
  - Primary CDR UNC Path
  - CDR Format
  - Primary CDR DSN
- Cisco Unified Communications Manager Release 6.0(1) supports the Call Monitoring and Call Recording features. No new CDR fields exist for these features. A CDR gets generated by using existing fields. For both monitoring and recording, the monitoring and recording calls have one-way media. The media fields remain empty for one side of the call for one-way media CDRs.

  Two new redirect reasons exist:
  - SS_RFR_RECORDING (value = 354)
  - SS_RFR_MONITORING (value = 370)

  Two new OnBehalfOf values exist:
  - Recording (value = 27)
  - Monitoring (value = 28)

  The destconversationID field of the Monitoring call CDR will match the agent call leg identifier in the CDR of the call that is monitored. This will link the monitored call CDR and the monitoring call CDR together.

  The origconversationID field of the two Recording call CDRs will match the agent call leg identifier in the recorded call CDR. This conversation ID will link the recorded call CDR and the CDRs that the recording calls generate.

- The Secure Conference feature includes a new CDR field, callSecuredStatus. CAR will use the existing call termination cause code value of 58 to show those calls that were cleared because they failed to meet the security level for the Secure Conference feature.
- AAC and iLBC comprise new codecs that are supported in Cisco Unified Communications Manager Release 6.0(1). For AAC calls, the codec specifies Media_Payload_AAC = 42, and the maxFramesPer Packet equals 1. For iLBC calls, the codec specifies Media_Payload_ILBC = 86.

  The release adds the following new bandwidth fields to the CDR:
  - origMediaCap_bandwidth: This represents an integer field that contains the audio bandwidth.
  - destMediaCap_bandwidth: This represents an integer field that contains the audio bandwidth.

- Cisco Unified Communications Manager Release 6.0(1) supports the Mobility feature. This feature includes Hand-In, Hand-Out, Cell Pickup, and Interactive Voice Response (IVR). No new CDR fields exist for these features, but a new OnBehalfOf field value and new Redirect Reason codes apply.

  One new OnBehalfOf value exists:

  - Mobility (value = 24)

  Four new Redirect Reason values exist:

  - SS_RFR_MOBILITY_HANDIN (value = 303)
  - SS_RFR_MOBILITY_HANDOUT (value = 319)
  - SS_RFR_MOBILITY_CELL_PICKUP (value = 335)
  - SS_RFR_MOBILITY_IVR (value = 399)
- Cisco Unified Communications Manager Release 6.0(1) supports the Intercom feature. No new CDR fields exist for this feature. For intercom, one-way audio exists, and the CDR reflects the one-way audio. For talk-back intercom, two-way audio exists, and the CDR reflects two-way audio. Because the Intercom feature requires a partition (intercom partition), you can use the existing CDR fields to identify intercom calls.
- The CDR for the Calling Party on Transfer consultation call of a Cisco Unity-initiated transfer changed in this release. The CDR of the consultation call will show that the original caller calls the transfer destination. Previously, the CDR showed that the Cisco Unity port called the transfer destination.
- Cisco Unified Communications Manager Release 6.0(1) reassigns the following OnBehalfOf code values:
  - Aar—current value = 25. Previous value specified 17.
  - Directed Call Park—current value = 26. Previous value specified 22.
- Table 4 shows the following changes occurred to existing CDR fields:

Table 4 Changes to Existing CDR Fields

Field Name	Description of Change
cdrRecordType	Add: value 1 = End call detail record (CDR)
origSpan	For calls that originate at a gateway, this field indicates the B-channel number of the T1 or PRI trunk where the call originated.
destSpan	For calls that are received at a gateway, this field indicates the B-channel number of the T1 or PRI trunk where the call is received.
origCallTerminationOnBehalfOf	New OnBehalfOf codes have been added.
destCallTerminationOnBehalfOf	New OnBehalfOf codes have been added.
origCalledPartyRedirectOnBehalfOf	New OnBehalfOf codes have been added.
lastRedirectRedirectOnBehalfOf	New OnBehalfOf codes have been added.
origCalledPartyRedirectReason	New OnBehalfOf codes have been added.
lastRedirectRedirectReason	New OnBehalfOf codes have been added.
joinOnBehalfOf	New OnBehalfOf codes have been added.

- The release adds value of 2 = CMR record to the cdrRecordType CMR field.

Where to Find More Information

- *Cisco Unified Communications Manager 4.2(1) Call Detail Record Definitions*
- *Cisco Unified Communications Manager 4.2(3) Call Detail Record Definitions*
- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*

Cisco Dialed Number Analyzer

The Cisco Unified Communications Manager Dialed Number Analyzer application enables users to test and diagnose a deployed Cisco Unified Communications Manager dial plan configuration, analyze the test results, and use the results to tune the dial plan.

Cisco Unified Communications Manager Dialed Number Analyzer includes the following enhancements in the Device Information section of the Results Summary:

Do Not Disturb (DND)

- DND Status—Enabled/Disabled based on the status of DND.
- DND Option—The option to have DND ringer on or off.
- DND Incoming Call Alert—No Beep/Flash notification/Beep only/Flash only depending on the type of alert that is chosen when the ringer is off.

Automated Alternate Routing (AAR)

- AAR Group Name—The AAR Group to which this device belongs.
- AAR Calling Search Space—The AAR Calling Search Space where this end device belongs.
- AAR Voice Mail Status—Enabled/Disabled. The AAR voice-messaging status of the device.
- AAR Destination Mask—The mask that is used to format the AAR destination.
- AAR Prefix Digits—The prefix digits that are used for automated alternate routing within this AAR group.

Intercom DN Pattern

- CSS—The calling search space of the intercom DN.
- Presence Group—The presence group to which the intercom DN belongs.

Where to Find More Information

- *Cisco Unified Communications Manager Dialed Number Analyzer Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*

Cisco Unified Communications Manager User Options Menu

The following enhancements occurred in the Cisco Unified CM User Options Menu (referred to as User Options) in release 6.0:

- The look and feel of the user options windows resembles the Cisco Unified Communications Manager Administration windows.
- The options are presented to the user in a menu instead of being listed on the main window. See Figure 1.
- The menu options include:
  - Device—includes Do Not Disturb configuration settings

Tip Access Help from the Device window. From the Device window, you can access the Cisco Unified IP Phone user guide and the information that describes the Cisco Unified CM User Options windows. In the Device window, click the **Download User Guide** link. This link displays if the Show Online Guide Option enterprise parameter is set to **True** in Cisco Unified Communications Manager Administration; in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameter**. When the PDF displays, refer to the Using the User Option Web Pages section.

  - User Settings
  - Directory
  - Personal Address Book
  - Fast Dials
  - Mobility Settings—includes access lists and remote destinations settings
  - Plugin
  - Download Online Documentation
- Directory enhancements include searching on multiple fields and displaying the device extension and the user telephone number.

Directory Enhancements

The following directory enhancements occurred in release 6.0 (see Figure 2):

- Directly accessed from User Options (versus manually entering a URL such as http://ccmserver/ccmuser/directory.asp)
- Search—last name, first name, user ID, extension, LDAP extension
- LDAP extension—ability to search on the users associated extension (versus the device extension)

  In releases 5.1(2) and 6.0, the directory contains the LDAP extension and the device extension. The LDAP extension column lists the number that the administrator enters in the Telephone Number field that is on the End User Configuration window. The extension column lists the directory number of the device that the administrator enters in the Directory Number Configuration window when configuring devices (this is the device that is associated to the user).

  In releases prior to 4.3, the extension column listed the Telephone Number (from the User Configuration window). In releases 5.0 and 5.1(1), the extension column listed the DNs that are associated with the device(s) that is associated with the user.

Figure 1 User Options Main Menu in Release 6.0

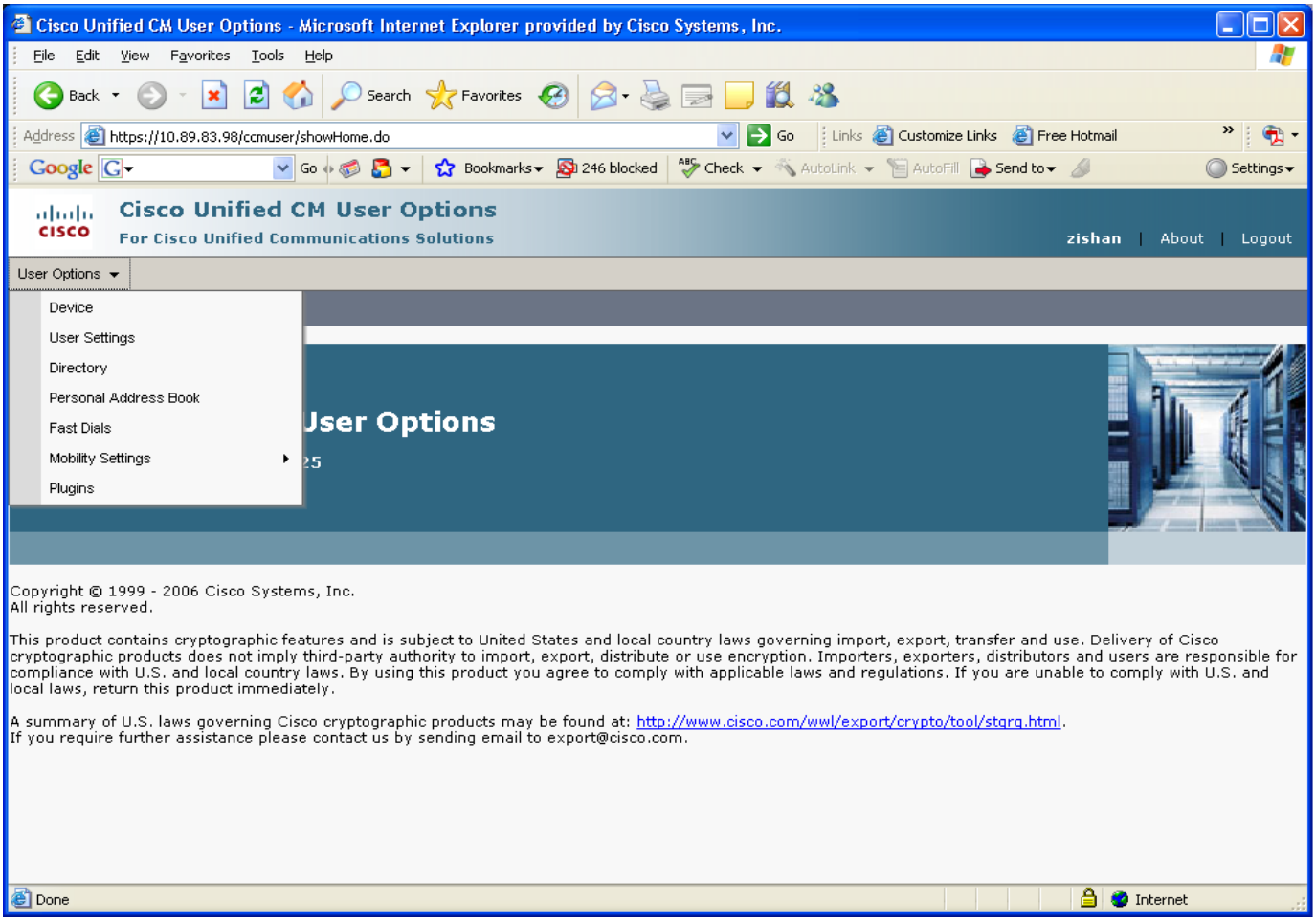
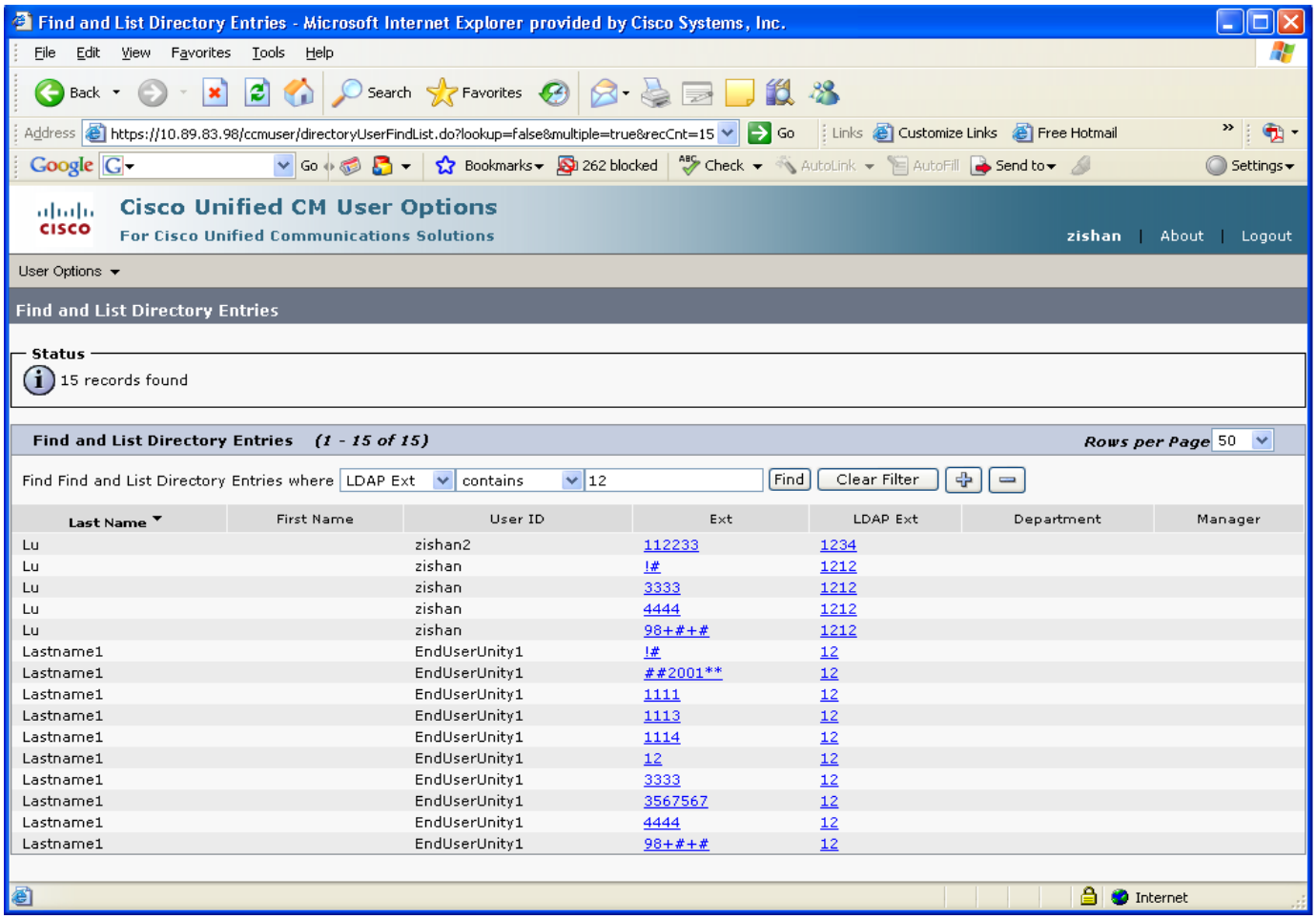


Figure 2 User Options Directory Search



Cisco Unified IP Phones

This section provides the following information:

Cisco Unified IP Phone 7931G (SCCP Only)

The system supports Cisco Unified IP Phone 7931G (SCCP only) on Cisco Unified Communications Manager Release 6.0 and later. The Cisco Unified IP Phone 7931G design meets the needs of businesses with moderate telephone traffic and specific call requirements. The Cisco Unified IP Phone 7931G supports IEEE 802.3af Power over Ethernet, security and other calling features. Dedicated hold, redial, and transfer keys facilitate call handling. Illuminated mute and speakerphone keys give a clear indication of speaker status.

Where to Find More Information

- *Cisco Unified IP Phone 7931G Installation Guide*
- *Cisco Unified IP Phone 7931G Phone Guide*
- *Cisco Unified IP Phone 7931G Administration Guide*

Wideband Settings

Cisco Unified Communications Manager Release 6.0 supports wideband codecs on handsets and headsets. Administrators can allow users to control configuration of the handset and/or headset by using their IP Phone User Interface. If the administrator disallows user control for one or both options, the administrator must configure the option(s) on Cisco Unified Communications Manager Administration Phone Configuration (or use the defaults). If the administrator allows user control (which is the default for both headset and handset wideband options), the user-configured values (both located in the User Preferences menu of the phone) take precedence over what is configured in Cisco Unified Communications Manager Administration.

Supported Cisco Unified IP Phones (SCCP and SIP)

7971G-GE, 7970G, 7961G-GE, 7961G, 7941G-GE, 7941G, 7911G, 7906G

Note The Cisco Unified IP Phones 7911G and 7906G support wideband settings on the handset only; the Cisco Unified IP Phone 7931G (SCCP only) supports wideband settings on the headset only.

For the availability of wideband handsets to accompany Cisco Unified IP phones, contact your Cisco representative or view product announcements on Cisco.com.

Supported Cisco Unified IP Phones (SCCP only)

7931G

Peer Firmware Sharing

The Peer Firmware Sharing feature adds support for image upgrade optimization for the Cisco Unified IP Phones. When enabled on a root IP phone, Peer Firmware Sharing designates the phone to make a request for an image file. This establishes a transfer hierarchy and transfers the firmware image file from the root IP phone, down to the other IP phones in the hierarchy.

Peer Firmware Sharing also allows for the designation of a remote logging machine, a Log Server, for debugging Peer Firmware Sharing firmware image update logs that are sent to the remote logging machine.

Peer Firmware Sharing remains disabled by default. To enable peer firmware sharing to upgrade firmware for a few phones, in Cisco Unified Communications Manager Administration,

choose **Device > Phone > Add New**. Then, from the Phone Configuration window, choose Peer Firmware Sharing from the Product Specific Configuration Layout section.

Supported Cisco Unified IP Phones (SCCP and SIP)

7971G-GE, 7970G, 7961G-GE, 7961G, 7941G-GE, 7941G, 7911G, 7906G

Supported Cisco Unified IP Phones (SCCP only)

7931G

BAT Considerations

To use Peer Firmware Sharing to upgrade firmware for many phones at once, set the Peer Firmware Sharing field in the Phone Template window of the BAT (**Bulk Administration > Phones > Phone Template**).

Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.0 Features

Table 5 lists Cisco Unified IP Phones that support new Cisco Unified Communications Manager 6.0 features. In addition, Cisco Unified Communications Manager 6.0 also supports release 4.2 features, including SIP support, as shown in Table 6.

Table 5 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.0 Features

Cisco Unified Communications Manager 6.0 Feature	Cisco Unified IP Phone Support	For more information, see
Programmable Line Keys	SCCP only: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7931G	Programmable Line Keys, page 48
Do Not Disturb (DND)	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7985G 7960G (via softkey) 7940G (via softkey) 7931G	Do Not Disturb, page 39
Intercom	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G SCCP only: 7931G 7914 Expansion Module	Intercom, page 42
Cisco Unified Communications Manager Assistant Enhancements	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7941G-GE SCCP only: 7985G 7960G 7940G	Cisco Unified Communications Manager Assistant, page 58

Table 5 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.0 Features (continued)

Cisco Unified Communications Manager 6.0 Feature	Cisco Unified IP Phone Support	For more information, see
Secure Conferencing	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7941G-GE SCCP only: 7960G 7940G 7931G **Note** See the Cisco Unified IP Phone 7931G Guide for limitations and restrictions.	Secure Conferencing, page 71 Secure Conference Icon, page 74
Wideband Settings **Note** The Cisco Unified IP Phones 7911G and 7906G support wideband settings on the handset only; the Cisco Unified IP Phone 7931G supports wideband settings on the headset only.	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7931G	Wideband Settings, page 88
Monitor & Record	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7941G-GE SCCP only: 7931G	Recording and Monitoring, page 68
Audible Message Waiting Indicator	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7931G	Audible Message Waiting Indicator, page 29

Table 6 Cisco Unified Communications Manager 4,x Features Ported to Cisco Unified Communications Manager 6.0

Cisco Unified Communications Manager 4.2 Features Ported to Cisco Unified Communications Manager 6.0	Cisco Unified IP Phone Support	For more information, see
Call Diagnostics and Voice Quality Metrics	SCCP and SIP: 7971G-GE 7970G/ 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G	Call Diagnostics and Voice Quality Metrics, page 30
Directed Call Park	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G 7914 Expansion Module	Directed Call Park, page 38
Log Out of Hunt Groups	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G 7912G 7905G	Log Out of Hunt Groups, page 46

Table 6 Cisco Unified Communications Manager 4,x Features Ported to Cisco Unified Communications Manager 6.0 (continued)

Cisco Unified Communications Manager 4.2 Features Ported to Cisco Unified Communications Manager 6.0	Cisco Unified IP Phone Support	For more information, see
Call Pickup Enhancements	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G 7912G 7905G	Call Pickup Notification, page 33
Conferencing Enhancements (ad hoc & chaining)	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G	Advanced Ad Hoc Conference, page 28

Table 6 Cisco Unified Communications Manager 4,x Features Ported to Cisco Unified Communications Manager 6.0 (continued)

Cisco Unified Communications Manager 4.2 Features Ported to Cisco Unified Communications Manager 6.0	Cisco Unified IP Phone Support	For more information, see
Hold Reversion	SCCP and SIP: 7971G-GE 7970G 7961G-GE 7941G-GE 7911G 7906G SCCP only: 7960G 7940G 7931G	Hold Reversion, page 41
MLPP Supplementary Services	SCCP and SIP: 7971G-G 7970G 7961G-GE 7961G 7941G-GE 7941G 7911G 7906G SCCP only: 7960G 7940G 7931G	Multilevel Precedence and Preemption (MLPP) Supplementary Services, page 66

Feature Support by Cisco Unified IP Phone and Protocol

For information about feature support differences between SCCP and SIP protocols, see the administration guide for your Cisco Unified IP Phone, “Feature Support by Protocol” section.

All Cisco Unified IP Phones

http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Cisco Unified IP Phone 7960G/7940G

Cisco Unified IP Phone 7960G/7940G Administration Guide for Cisco Unified Communications Manager 5.0 (SIP)
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Cisco Unified IP Phone 7905G/7912G

Cisco Unified IP Phone 7905G/7912G Administration Guide for Cisco Unified Communications Manager 5.0 (SIP)
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Call Forward All Loop Prevention Message Changes

Changes for the following error messages that display on the phones for Call Forward All (CFA) loop prevention occurred:

- When a user activates CFA from a phone, resulting in a CFA loop:
  - Original error message: "Call Forward Loop"
  - New error message: "CFwdAll Loop Detected"
- When a CFA request exceeds the number of allowed hops (also when a user activates CFA from the phone):
  - Original error message: "Forward Hops Exceeded"
  - New error message: "CFwdAll Hops Exceeded"

Cisco and Third-Party APIs

This following sections describe new features and changes that are pertinent to this release of the Cisco Unified Communications Manager APIs and the Cisco extensions to third-party APIs.

- Cisco Unified Communications Manager Developers Guide, page 95
- Cisco Unified Communications Manager Data Dictionary, page 97
- Cisco Unified JTAPI Developers Guide, page 100
- Cisco Unified JTAPI Developers Guide for Release 4.2(3), page 104
- Cisco Unified JTAPI Developers Guide for Release 4.2(1), page 105
- Cisco Unified TAPI Developers Guide, page 105
- Cisco Unified TSP Enhancements for Release 4.2(1), page 107
- SCCP Messaging Guide for Cisco Unified Communications Manager 6.0(1), page 108
- SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(4), page 109
- SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(2), page 110
- SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(1), page 110

Cisco Unified Communications Manager Developers Guide

The *Cisco Unified Communications Manager Developers Guide* describes the following APIs:

- AXL Programming, page 95
- AXL Serviceability Programming, page 97
- Extension Mobility API, page 97
- Cisco Web Dialer, page 97

AXL Programming

The following major changes occurred in the AXL APIs for Release 6.0(1):

- Introduced AXL schema versioning to improve backward compatibility.
- Added a total of 76 new APIs.
- Added the following three fields to the AXL device/line create APIs:

  - ASCII Display (internal call ID)
  - Secondary Calling Search Space for Forward All
  - Unattended Port
- Added new AXL APIs and attributes to support mobility provisioning and added optional attributes to existing AXL objects.
- Added the new tag cfaCSSPolicy to the Line API.
- Added APIs to support Credential Policy.
- Updated the database schema.

  Some fields that were removed from the database have been deprecated in AXL. Annotation has been added for such fields.

  Code that uses the AXL APIs executeSQLQuery and updateSQLquery may need to be updated.
- Changed the default value of the AXL service parameter, so it allows a valid namespace to be returned in AXL responses.
- Added a new service parameter, EnableAXLEncodingInfo, to better support languages other than English.
- The AXL API now considers PKID with or without curly brackets as a valid input.

The following AXL API calls changed since the previous release. These changes might require changes to existing user code that makes use of them:

addCallPickupGroup	addConferenceBridge	addCSS
addDevicePool	addDeviceProfile	addFACInfo
addGatewayEndpoint	addH323Phone	addH323Trunk
addLine	addMGCP	addPhone
addRegion	addRoutePartition	addSIPTrunk
addUser	addVoiceMailPort	doAuthenticateUser
getCallPickupGroup	getCMCInfo	getConferenceBridge
getCSS	getDevicePool	getDeviceProfile
getFACInfo	getGatewayEndpoint	getH323Phone
getH323Trunk	getLine	getMGCP
getPhone	getRegion	getRoutePartition
getSIPTrunk	getUser	getVoiceMailPort
removeCMCInfo	removeFACInfo	updateAppUser
updateCallPickupGroup	updateCMCInfo	updateConferenceBridge
updateCSS	updateDevicePool	updateDeviceProfile
updateFACInfo	updateGatewayEndpoint	updateH323Phone
updateH323Trunk	updateLine	updatePhone
updateRegion	updateRegionMatrix	updateRoutePartition
updateSIPTrunk	updateUser	updateVoiceMailPort

AXL Serviceability Programming

The following changes occurred in the AXL Serviceability APIs for Cisco Unified Communications Manager Release 6.0(1):

- Added the new API getProductInformationList as part of ControlCenterServicePort. This API provides information about products that are installed on a given server.
- Upgraded the SOAP server to AXIS 1.4.
- Added SOAP API support for password expiration and lockout.
- Added a SOAP authorization timed finite cache to improve performance for SOAP applications that do not maintain a https session.
- Made the API available in a variety of different installation configurations of the Cisco Unity and Cisco Unified Communications Manager products.

The updated manual also includes more detailed information about error codes.

Extension Mobility API

Rearchitected Cisco Extension Mobility in Cisco Unified Communications Manager Release 6.0(1) improves login/logout performance. The new extension mobility architecture also migrated to support the Call Processing User Facing Feature architecture.

The following list describes the Extension Mobility API enhancements for Cisco Unified Communications Manager Release 6.0(1):

- The Extension Mobility rearchitecture creates a new table, ExtensionMobiltyDynamic, that supports simple timestamp conflict resolution and is writable on all nodes in the system.
- To support database resiliency, some fields moved to their own tables, so they can be updated locally and replicated in a fully meshed topology. This will break direct SQL access to columns in the database that moved from one table to another.
- Loss of connectivity to the publisher server will no longer prohibit Extension Mobility login/logout from completing successfully.

Cisco Web Dialer

The following changes occurred to Cisco Web Dialer for Cisco Unified Communications Manager 6.0(1):

- The makeCallSoap API includes a new, optional service parameter: “Apply Application Dial Rules on SOAP Dial Request.” This service parameter False by default; if this parameter is True, the destination gets transformed according to the dial rules.
- SOAP messages now use HTTPS. The updated WSDL reflects the changed port number.

Cisco Unified Communications Manager Data Dictionary

The following sections describe the differences between Cisco Unified Communications Manager Releases 6.0 and 5.1 and Releases 6.0 and 5.0(4).

Differences Between 6.0(1) and 5.1(1)

Cisco Unified Communications Manager 6.0(1), and not Cisco Unified Communications Manager 5.1(1), includes the following tables:

- applicationusercapfmapdynamic
- blfdirectedcallpark

- blfspeeddial
- callerfilterlist
- callerfilterlistmember
- callforwardalloverride
- callforwarddynamic
- commondeviceconfig
- commonphoneconfig
- credential
- credentialdynamic
- credentialhistory
- credentialpolicy
- credentialpolicydefault
- devicehlogdynamic
- devicemobilitydynamic
- devicemobilitygroup
- devicemobilityinfo
- devicenumplanmapendusermap
- devicenumplanmapremdestmap
- devicepooldevicemobilityinfomap
- deviceprivacydynamic
- dnddynamic
- endusercapfmapdynamic
- extensionmobilitydynamic
- ivruserlocale
- numplandcpsyn
- physicallocation
- recordingdynamic
- recordingprofile
- remotedestination
- softkeytemplatedefault
- typecallerfiltermask
- typecredential
- typecredentialuser
- typedndoption
- typelossynetwork
- typenodeusage
- typeoutboundcallrollover
- typepartitionusage

- typepickupnotification
- typerecordingflag
- typerevertpriority
- replicationdynamic

Cisco Unified Communications Manager 5.1(1) and not Cisco Unified Communications Manager 6.0(1), includes the following tables:

- busylampfield
- commonprofile
- typezzkpml

For detailed information on tables and the fields in those tables that differ in Cisco Unified Communications Manager 6.0(1) and Cisco Unified Communications Manager 5.1(1), refer to Section 4.1.3 in the *Cisco Unified Communications Database Dictionary for Release 6.0(1)*.

Differences Between 6.0(1) and 5.0(4)

Cisco Unified Communications Manager 6.0(1) and not Cisco Unified Communications Manager 5.0(4), includes the following tables:

- applicationusercapfmapdynamic
- blfdirectedcallpark
- blfspeeddial
- callerfilterlist
- callerfilterlistmember
- callforwardalloverride
- callforwarddynamic
- commondeviceconfig
- commonphoneconfig
- credential
- credentialdynamic
- credentialhistory
- credentialpolicy
- credentialpolicydefault
- devicehlogdynamic
- devicemobilitydynamic,
- devicemobilitygroup
- devicemobilityinfo
- devicenumplanmapendusermap
- devicenumplanmapremdestmap
- devicepooldevicemobilityinfomap
- deviceprivacydynamic
- dnddynamic

- endusercapfmapdynamic
- extensionmobilitydynamic
- ivruserlocale
- numplandcpsyn
- physicallocation
- pilotuserdata
- recordingdynamic
- recordingprofile
- remotedestination
- softkeytemplatedefault
- typecallerfiltermask
- typecredential
- typecredentialuser
- typedndoption
- typelossynetwork
- typenodeusage
- typeoutboundcallrollover
- typepartitionusage
- typepickupnotification
- typerecordingflag
- typerevertpriority
- replicationdynamic

Cisco Unified Communications Manager 5.0(4) and not Cisco Unified Communications Manager 6.0(1), includes the following tables:

- busylampfield
- commonprofile
- typezzkpml

For detailed information on tables and the fields in those tables that differ in Cisco Unified Communications Manager 6.0(1) and Cisco Unified Communications Manager 5.0(4), refer to Section 4.2.3 in the *Cisco Unified Communications Database Dictionary for Release 6.0(1)*.

Cisco Unified JTAPI Developers Guide

The following sections describe the JTAPI enhancements for Cisco Unified Communications Manager 6.0(1). Refer to the *Cisco Unified JTAPI Developers Guide* for a complete description of these enhancements.

- Recording and Silent Monitoring
- Intercom
- Arabic and Hebrew Language Support
- Do Not Disturb

- Secure Conferencing
- SIP Phone Support
- Cisco Unified IP Phone 7931G (SCCP Only) Interaction
- Version Format Change
- Querying the Calling Party IP Address
- Multilevel Precedence and Preemption (MLPP) Support
- Non-Controller Adding of Parties to Conferences
- Conference Chaining
- Forwarding on No Bandwidth & Unregistered DN
- Directed Call Park
- Voice MailBox Support
- Privacy On Hold
- CiscoRTPHandle Interface on Cisco RTP Events
- Hold Reversion
- Backward Compatibility

Recording and Silent Monitoring

This feature lets applications record and silently monitor calls. The caller represents the end point, which calls or receives a call from the monitor target or the recording initiator. The monitor target represents the party to monitor (the agent), and the monitoring party specifies the monitor initiator (the supervisor).

The recording feature lets applications record conversations on any observed address. The following three available recording configurations exist:

- No recording
- Automatic recording
- Application-controlled recording

Intercom

The Intercom feature allows one user to call another user and have the call answered automatically with one-way media from the caller to the called party, regardless of whether the called party is busy or idle. The called user can press the talkback softkey (unmarked key) on their phone display, or the called user can invoke the join() JTAPI API, which is provided on TerminalConnection, to start talking to the caller. Only a specially configured intercom address on the phone can initiate an intercom call. JTAPI creates a new type of address object named CiscoIntercomAddress for intercom addresses that are configured on the phone. The application can get all the CiscoIntercomAddress that are present in the provider domain by calling the interface getIntercomAddresses () on CiscoProvider.

Arabic and Hebrew Language Support

This version of the Cisco JTAPI supports the Arabic and Hebrew languages, which users may select during installation and in the Cisco JTAPI Preferences user interface.

Do Not Disturb

Do-Not-Disturb capability gives phone users the ability to go into a Do Not Disturb (DND) state on the phone when they are away from their phones or do not want to answer the incoming calls. The DND softkey enables and disables this feature.

Secure Conferencing

This feature informs applications whether a call is secure, allowing for secure conference calls. When the overall security status of the call changes, secure conferencing provides applications with a notification in the form of an event on the call. Applications can query the security status of the call by using a new interface on CiscoCall.

SIP Phone Support

In release 5.0, JTAPI supported an initial feature set on SIP phones. The 6.0 release adds support for Park and Unpark on SIP phones.

Cisco Unified IP Phone 7931G (SCCP Only) Interaction

You can configure the Cisco Unified IP Phone 7931G in two modes:

- NoRollOver
- RollOver (across the same DN or across different DNs)

When the Cisco Unified IP Phone 7931G is configured in NoRollOver mode, it operates like a regular SCCP phone, and, in this mode, transfers or conferences cannot be made across the different addresses. JTAPI supports controlling and monitoring of a Cisco Unified IP Phone 7931G when it is configured in NoRollOver mode.

In RollOver mode, the Cisco Unified IP Phone 7931G supports transfer or conference across different addresses. In this mode, JTAPI does not allow controlling and monitoring of the Cisco Unified IP Phone 7931G. If a Cisco Unified IP Phone 7931G that is configured in RollOver mode transfers or conferences to JTAPI-controlled addresses, JTAPI applications will not see a common controller in the final and the consult call. This would provide different behavior to the JTAPI application. Depending on how the JTAPI application is processing information that is provided in events, applications may require changes to handle JTAPI events for this transfer or conference scenario.

Version Format Change

In release 6.0, the Cisco JTAPI version changes from a 4-digit format to a 5-digit format that is similar to the format that Cisco Unified Communications Manager uses. The JTAPI version will remain similar to the Cisco Unified Communications Manager version. New interfaces let applications get the extended version number.

Querying the Calling Party IP Address

Extensions to CallCtlConnOfferedEv and RouteEvent provide a method for retrieving the IP address of the calling party. This feature provides the calling party IP address to the destination side of basic calls, consultation calls for transfer and conference, and basic redirect and forwarding. The system does not support other scenarios and feature interactions, including those where the calling party changes. This feature only supports IP phones as calling party devices, although IP address of other calling devices may also be provided.

Multilevel Precedence and Preemption (MLPP) Support

Cisco Unified Communications Manager enables the use of supplementary services by phones that are configured for MLPP. Cisco Unified Communications Manager does this by maintaining the precedence level for calls.

Non-Controller Adding of Parties to Conferences

Any party in a conference can now add participants into the conference. In previous releases, only the conference controller could add participants.

Conference Chaining

The conference chaining feature lets applications join two separate conference calls together. JTAPI applications see chained conference calls represented as two separate calls. When conference calls are chained, JTAPI creates a new connection for the conference chain and provides the CiscoConferenceChainAddedEv event on CallCtlCallObserver. When the conference chain is removed from the call, JTAPI disconnects the conference chain connection and provides the CiscoConferenceChainRemovedEv event on CallCtlCallObserver. From CiscoConferenceChainAdded/RemovedEv, applications can obtain CiscoConferenceChain, which provides a link for all the conference chain connections.

Forwarding on No Bandwidth & Unregistered DN

This feature enhances the forwarding logic to handle the No Bandwidth & Unregistered DN cases.

Directed Call Park

This feature allows the user to park a call by transferring the call to a user-selected park code. When the system transfers a call to a directed call park DN (dparked), the application sees a connection that is created for directed call park DN, and the call control connection state specifies CallControlConnection.QUEUED. The system delivers CiscoTransferstart and end events. An application can use the new interface on CiscoConnection to get the prefix code that is needed to unpark the call.

Voice MailBox Support

This feature exposes voice mailbox numbers, which let Cisco Unified Communications Manager JTAPI applications forward calls from a directory number to the correct voice mailbox. To support this feature, JTAPI exposes voice mailbox numbers for the called party, the lastRedirected party, and the originalCalled party on CiscoPartyInfo. In prior releases, Cisco Unified Communications Manager JTAPI did not expose voicemailbox fields to applications, so JTAPI voicemailbox applications could not determine whether a voicemailboxmask was configured for a voicemail profile, which could result in a voicemailbox number that differs from the directory number.

Privacy On Hold

This feature enhances the privacy of private held calls. When privacy is enabled, only the phone that placed a call on hold can retrieve that call, and the calling name and number do not display. The feature provides a shared address with the ability to determine whether other shared addresses may barge in to a call. When privacy is enabled, other shared address cannot barge in to the call.

In prior releases, if Privacy is enabled and the call is put on hold, all TerminalConnections will be in TermConnHeld state, and any other shared Address terminalConnection can unhold the call.

CiscoRTPHandle Interface on Cisco RTP Events

Enhancements allow the following interfaces to allow applications to get a CiscoRTPHandle from the events:

- CiscoRTPInputStartedEv
- CiscoRTPInputStoppedEv
- CiscoRTPOutputStartedEv
- CiscoRTPOutputStoppedEv

CiscoRTPHandle represents the caller ID of the call in Cisco Unified Communications Manager and the same as long as the call is active on the terminal. At any particular terminal/address, although the call and the associated GCID can change, CiscoRTPHandle will remain constant.

Hold Reversion

The Hold Reversion feature provides applications with a notification, when Cisco Unified Communications Manager notifies an address about the presence of a held call, when the call has been ONHOLD for a certain time. Applications receive this notification as the CiscoCallCtlTermConnHeldReversionEv call control terminal connection event on their call observers on the particular address that has put the call ONHOLD. The system provides this notification only once for the applications for the held call.

To receive this event, applications must add a call observer to the address.

Backward Compatibility

This release of JTAPI provides backward compatibility with applications that were written for release 5.1. Be aware that upgrading the CiscoJtapiClient is not mandatory. Applications must upgrade to 6.0 CiscoJTAPIClient only if they want to use the new features that are introduced in release 6.0. The updated *Cisco Unified Communications Manager JTAPI Developers Guide* contains a new section that explains in detail the backward compatibility features of Cisco JTAPI.

Cisco Unified JTAPI Developers Guide for Release 4.2(3)

Cisco Unified JTAPI previously got upgraded whenever Cisco Unified Communications Manager was upgraded. With the 4.2 versions of Cisco Unified Communications Manager, Cisco Unified JTAPI does not need to be upgraded if your application does not use any new features that are introduced in the 4.2 release. Cisco JTAPI for Cisco Unified Communications Manager Release 4.1 will work with Cisco Unified Communications Manager Release 4.2, if the 4.2 features are not enabled.

Cisco Unified JTAPI from the 4.2 versions of Cisco Unified Communications Manager does not work with earlier versions of Cisco Unified Communications Manager. If Cisco Unified Communications Manager is downgraded from version 4.2 to version 4.1, you need to downgrade Cisco Unified JTAPI as well.

Cisco Unified JTAPI for Cisco Unified Communications Manager Release 4.2(3) introduced the following new features:

Advanced Ad Hoc Conference

You can disable this feature, which is backward compatible, as long as the feature is disabled through a systemwide service parameter called Advanced Ad hoc Conference. When the feature is enabled and conference chaining is done on application-controlled devices, the system might require applications to make changes to handle conference chaining events.

Refer to the *Cisco Unified Communications Manager JTAPI Developers Guide for Release 4.2(3)* for the complete details of advanced ad hoc conference implementation in this release.

Hold Reversion

Cisco Unified Communications Manager supports hold reversion on Cisco SCCP IP Phones. The Hold Reversion feature only applies to the user hold; it does not apply to the network hold or hold that results from a feature invocation.

After a holding party puts a call on hold for a certain time, the holding party receives a hold reversion notification ring and a prompt display message.

Refer to the *Cisco Unified Communications Manager JTAPI Developers Guide for Release 4.2(3)* for the complete details of advanced ad hoc conference implementation in this release.

Cisco Unified JTAPI Developers Guide for Release 4.2(1)

The following list describes the changes to Cisco JTAPI for Cisco Unified Communications Manager 4.2(1):

- Cisco Communications Manager version compatibility—You need not upgrade Cisco JTAPI version 2.1(x) when upgrading to Cisco Communications Manager 4.2(1), unless you want to use features that are new in Cisco JTAPI 2.2. Previously, you were required to upgrade Cisco JTAPI when upgrading Cisco Communications Manager.

  If you downgrade Cisco Unified Communications Manager 4.2 to release 4.1, you must also downgrade Cisco JTAPI from version 2.2 to version 2.1(x).

- Forwarding on No Bandwidth and Unregistered—Enhances the forwarding logic to handle the No Bandwidth and Unregistered cases:
  - No Bandwidth: When a call cannot be delivered to a remote destination due to no bandwidth, the call gets rerouted to the AAR Destination Mask or Voice Mail. The user makes these configuration changes from the Directory Number Configuration window of the Cisco Unified Communications Manager GUI.
  - Unregistered DN: When a call is targeted to an unregistered DN, the call gets delivered to a DN that is configured for Call Forward on No Answer (CFNA), as in previous releases.

- Transfer Invoked Directed Call Park—Allows the user to park a call by transferring the call to a user-selected park code.

  When a call is transferred to a directed call park DN (dparked), the application sees a connection that is created for directed call park DN, and the call control connection state specifies CallControlConnection.QUEUED. CiscoTransferstart and end events get delivered. An application can use the new interface on CiscoConnection to get the prefix code that is needed to unpark the call.

- VoiceMailBox Support—Exposed voice mailbox numbers allow CTI applications to forward calls from a directory number to the correct voice mailbox.

- Privacy On Hold—Enhances the privacy of private, held calls. Only the phone that placed a call on hold can retrieve that call, and the calling name and number do not display.

For information about third-party and SDK applications, refer to the *Cisco Unified Communications Manager JTAPI Developers Guide for Release 4.2(1)*.

Cisco Unified TAPI Developers Guide

The following sections describe the TAPI enhancements for Cisco Unified Communications Manager Release 6.0(1). Refer to the *Cisco Unified TAPI Developers Guide* for a complete description of these enhancements.

- Intercom Support
- Secure Conferencing Support
- Additional Features Supported on SIP Phones
- Silent Monitoring
- Call Recording
- Conference Enhancements
- Arabic and Hebrew Language Support
- Silent Install Support

- Do Not Disturb
- Translation Pattern

Intercom Support

The Intercom feature allows one user to call another user and have the call automatically answered with one-way media from the caller to the called party, regardless of whether the called party is busy or idle. TSP exposes the intercom line indication and intercom speeddial information in DevSpecific of LineDevCap. The application can retrieve the information by issuing LineGetDevCaps. In the DevSpecific portion, TSP provides information that indicates (DevSpecificFlag = LINEDEVCAPSDEVSPECIFIC_INTERCOMDN) whether this is the intercom line. Users can retrieve the intercom speeddial information in the DevSpecific portion after the partition field.

Secure Conferencing Support

In previous releases, the security status of each call remained the same as the status for the call between the phone and its immediately connected party, which is a conference bridge in the case of a conference call. No secured conference resource existed, so secure conference calls were not possible. This release supports a secured conference resource to enable secure conferencing. TAPI passes the overall call security status to the application.

Additional Features Supported on SIP Phones

The current release extends support for SIP phone features.

- PhoneSetLamp (but only for setting the MWI lamp)
- PhoneSetDisplay
- PhoneDevSpecific (CPDST_SET_DEVICE_UNICODE_DISPLAY)
- LineGenerateTone
- Park and UnPark
- The LINECALLREASON_REMINDER reason for CallPark reminder calls
- PhoneGetDisplay (but only after a PhoneSetDisplay)

Silent Monitoring

Silent monitoring lets a supervisor eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session. TSP provides a start monitoring type in the line DevSpecific request to allow applications to monitor calls on a per-call basis.

Call Recording

Call recording provides two ways of recording the conversation between the agent and the customer:

- Automatic recording of all calls
- Application-invoked selective call recording

Conference Enhancements

This release includes the following conference enhancements:

- Allowing a noncontroller to add another party into an ad hoc conference.
- Allowing multiple conferences to be chained.
- Be aware that these features are only available if the Advanced Ad hoc Conference service parameter is enabled in the Cisco CallManager service.

Arabic and Hebrew Language Support

This release supports the Arabic and Hebrew languages. Users can select these languages during installation and also in the CiscoTSP settings user interface.

Silent Install Support

The CiscoTSP installer now supports silent install, silent upgrade, and silent reinstall from the command prompt. Users do not see any dialog boxes during the silent installation.

Do Not Disturb

The Do Not Disturb (DND) feature lets phone users go into a Do Not Disturb state on the phone when they are away from their phone or simply do not want to answer incoming calls. The phone softkey DND enables and disables this feature. Cisco TSP makes the following phone device settings available for DND functionality:

- DND Option: None/CallReject/Ringer off
- DND Incoming Call Alert: beep only/flash only/disable
- DND Timer: A value between 0-120 minutes. It is a period in minutes to remind the user that DND is active.
- DND enable and disable

This feature applies to phones and CTI ports. It does not apply to route points.

Translation Pattern

TSP does not support the Translation Pattern because it may cause a dangling call in a conference scenario. The application needs to clear the call to remove this dangling call or simply close and reopen the line.

Cisco Unified TSP Enhancements for Release 4.2(1)

The following section describes the Cisco Unified TSP enhancements for Cisco Unified Communications Manager 4.2(1).

Cisco Unified Communications Manager Version Compatibility

You need not upgrade Cisco TSP when you upgrade to Cisco Unified Communications Manager 4.2(1), unless you want to use features that are new for the 4.2(1) release. Previously, the system required you to upgrade Cisco TSP when you upgrade Cisco Unified Communications Manager.

Windows 2003 Support

Cisco TSP now gets supported on Windows 2003.

Call Forwarding

Cisco Unified Communications Manager 4.2(1) provides enhancements to the forwarding and Automated Alternate Routing (AAR) logic to redirect calls that cannot be connected due to no bandwidth or an unregistered directory number.

No Bandwidth—In this scenario, a call comes in from a gateway at the central site (Centralized CallManager Configuration) for a phone at a remote site. Previously, if AAR was enabled, and insufficient bandwidth existed to deliver the call to the remote site, Cisco Unified Communications Manager rerouted the call through PSTN or other network by using an alternate number that was derived from the external phone number mask. The AAR cannot redirect the call to an alternate destination (for example, a cell phone or voice-messaging system).

Now, you can configure an alternate call destination or direct the call to a voice-messaging system. AAR handles no bandwidth calls and reroutes them to the AAR Destination Mask or to a voice-messaging system.

TAPI applications receive the LINECALLREASON_FWDBUSY call reason in this scenario.

Unregistered Phone—In this scenario, a call that is placed to a DN that remains unregistered. Previously, the CFNA (Call Forward No Answer) forwarding logic handled that call.

Now, Cisco Unified Communications Manager can determine whether the call is not answered or whether the target DN is unregistered. This feature adds a new call forwarding type CFUR (Call Forward Unregistered) to handle the calls that are targeted to an unregistered DN.

TAPI applications receive the LINECALLREASON_FWDNOANSWER call reason in this scenario.

Privacy on Hold

A shared line cannot retrieve a held call on which privacy is enabled. However, a shared line can retrieve the call if its privacy mode is disabled.

When a privacy enabled call is put on hold, Cisco TSP reports the call state as CONNECTED INACTIVE for calls on shared lines.

Directed Call Park

This feature allows you to select a park code at which to park a call. Previously, you could not select the park code; it was assigned automatically.

Cisco TSP sends the prefix code to the application as part of dwConnectedIDName in the format “Park Number:<PrefixCode><DParkDN>”. Applications can use <PrefixCode> and <DParkDN> to unpark a parked call.

When the call is parked, unparked, or reverted for the directed call park, the call reasons that are reported by Cisco TSP the same as for the normal park cases:

- LINECALLREASON_UNPARK gets reported when the call is unparked.
- LINECALLREASON_REMINDER gets reported when call park reversion happens.

Where to Find More Information

For information about third-party and SDK applications, refer to the *Cisco Unified Communications Manager TAPI Developer Guide for Release 4.2(1)*.

SCCP Messaging Guide for Cisco Unified Communications Manager 6.0(1)

This release includes three new versions of the SCCP messaging protocol. This version of the *Skinny Client Control Protocol (SCCP) Messaging Guide for Cisco Unified Communications Manager 6.0(1)* documents all three versions:

- Version 12 provides the comprehensive update for Release 6.0(1) and includes all the new features.
- Version 11 enhances Version 9 with secure icon control.
- Version 10 enhances Version 9 with conversion of inband DTMF tones to RFC 2833/OOB. Version 10 represents a limited-distribution software release.

Note Be aware that versions 10 and 11 are independent; version 11 does not include the inband DTMF tone conversion feature, and version 10 does not include secure icon control.

Two new messages exist, and changes occurred to several existing messages.

Inband DTMF Tone Conversion to and from RFC2833 via Transcoder (Version 10)

The transcoder can now convert inband DTMF tones to RFC2833/OOB (OUT OF BAND). The IP-IP GW invokes the transcoder, which is acting as the SCCP server. A new field enables inband DTMF tone to RFC2833 conversion on media streams. Consider this field as required in StationOpenReceiveChannelMessage and StationStartMediaTransmissionMessage.

Call Agent Security Icon Control (Version 11)

In earlier versions of SCCP, the call agent could not indicate to the station that a particular call is encrypted. This forced the endpoints to look at their currently active streams to determine whether they were using SRTP instead of RTP. Version 11 of the SCCP protocol allows endpoints that already support SRTP to participate in secured conferences without supporting the other Version 12 enhancements.

Silent Monitor & Record

Silent monitoring lets a supervisor eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Call recording lets system administrators or other authorized personnel archive conversations between the agent and the customer.

Intercom

The Intercom feature lets one user call another and have the call be answered automatically with one-way media from the caller to the called party, regardless whether the called party is busy or idle. The called party can optionally talk back to the caller, which creates a two-way media connection.

Do Not Disturb (DND)

The Do Not Disturb feature lets phone users specify a Do Not Disturb (DND) setting on their phone when they are away or do not want to answer incoming calls.

Mobility

The Mobility feature lets Cisco Unified Communications Manager support enterprise mobility functionality such as single number reach, desk pickup, cell pickup, IVR, and dual-mode phones.

Line-Feature Buttons for Cisco Unified IP Phones 7931G (SCCP Only)

The Cisco Unified IP Phone 7931G hardware implements three hardware feature buttons. The Cisco Unified IP Phone 7931G and TNP phone firmware also permits configuring various call features (in addition to the existing Speed Dial, BLF Speed Dial, Service URL, and Privacy features) on their line buttons. In previous Cisco Unified Communications Manager releases, no support existed for the mapping of these hardware buttons and these new line-feature buttons.

SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(4)

Cisco Unified Communications Manager Release 5.0(4) included the following SCCP messaging changes and new features.

- Added a description of the featureStatus field for the SsGenericStimulusFeature usage.
- Corrected the StationRegisterAckMessage to include the alignmentPadding field, which is used to make the message size a multiple of 4 bytes, and the MaxProtocolVersion field, which is the highest protocol version that Cisco Unified Communications Manager can support to the SCCP endpoint.
- Added description of the StimulusFeature Call Flow.

SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(2)

No new SCPP messaging features or enhancements exist in Cisco Unified Communications Manager Release 5.0(2) other than product name changes.

SCCP Messaging Guide for Cisco Unified Communications Manager 5.0(1)

Cisco Unified Communications Manager Release 5.0(1) includes the following new SCCP messaging features:

RFC2833 Support

The following message changes for RFC2833 support in SCCP messages occurred:

- Addition of new Media payload type that affects the content of StationCapabilitiesRes and StationUpdateCapabilities.
- StationOpenReceiveChannel
- StationStartMediaTransmission
- StationSubscribeDtmfPayloadReqMessage
- StationUnSubscribeDtmfPayloadReqMessage

Presence/BLF SpeedDial Support

The enhanced SpeedDial feature includes BLF status. An SCCP endpoint with BLF SpeedDial enabled can subscribe to the BLF status of the SpeedDial DN. If the subscriber is authorized, the status displays.

This feature uses the existing StationFeatureStatReqMessage and StationFeatureStatMessage. No new or impacted SCCP messages exist for Presence/BLF SpeedDial Support.

Presence/BLF Call History Support

Enhanced Call History, including missed calls, received calls, and placed calls, includes BLF status. When an SCCP endpoint user views the call history, the BLF status of each call entry displays if the subscription for the BLF status is authorized.

RSVP Agent Support

This release added RSVP Agent support, a new feature. Some SCCP messages were modified to support QoS (RSVP Agent).

Support for Serviceability

This change requires the device MAC address in the StationRegisterMessage. Originally, the device name field in the StationRegisterMessage was MAC address-based, and the device name format started as alphabetic characters and ended with the MAC address. Now, because the MAC address is a separate field in this message, the device name does not need to be MAC address-based, which eases installation and maintenance. StationRegisterMessage represents the only impacted SCCP message.

K-factor Voice Quality Diagnostic Data Report

This feature allows the customer to track Voice Quality (VQ) metrics in compliance with Service Level Agreements (SLA). The existing statistics that are reported by both the IP phones (SCCP) at the end of each call (the number of dropped packets/octets, jitter, and so on) proved not sufficient for this purpose. The release added the following nine VQ metrics: 1) Cum Conceal Ratio, Interval Conceal Ratio, Max Conceal Ratio, Conceal Second, Severely Conceal Second, MOS Listening Quality K-factor, MOS

Listening Quality K-factor Min, MOS Listening K-factor Max, and MOS Listening Quality K-factor Average. For the SCCP IP phones, newly introduced VQ data gets added in the existing StationConnectionStatisticsResMessage SCCP message.

SCCP Modification for Media Path

Currently, both Cisco Unified Communications Manager and SCCP endpoints control softkey set mask. Firmware controls the media-path-related softkey(s) enable/disable; however, firmware does not have complete knowledge of the call status. The softkey mask-controlling logic moved to Cisco Unified Communications Manager. In SCCP Protocol Version 8, StationHeadsetStatusMessage does not get recommended to report headset status. Instead, use StationMediaPathEventMessage.

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of severity level 1, 2, and 3.

Caveats describe unexpected behavior on a Cisco Unified Communications Manager 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 6.0(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/action.do?hdnAction=searchBugs.

This section includes the following topics:

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Log on with your Cisco.com user ID and password.

Note If you are looking for information about a specific caveat, enter the ID number in the "Search for bug ID:" field and click **Go**.

Step 2 From the Select Product Category drop-down box, choose "Voice and Unified Communications."

Step 3 From the Select Product drop-down box, choose "Cisco Unified Communications (CallManager)."

Step 4 In the Software Version, Version drop-down list, choose the major release of Cisco Unified Communications Manager for which you want the caveats (for example, 5.0, 6.0, etc.).

Step 5 Under Advanced Options, choose "Use custom settings for severity, status, and others."

a. In the information that displays, click (to "uncheck") the Fixed check box.

b. From the Modified Date drop-down list, choose "Any Time."

Step 6 Click **Search**.

Note You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 112.

Note For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects that are being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 111.

Step 2 Click the **Save Search** button that displays at the bottom of the window.

The Save Search Setting window displays.

Step 3 In the Search Name field, enter a name for the saved search.

Step 4 In the Place in Group section, you can:

- Click the **Existing group**: radio button and choose an existing group name from the drop-down list box.
- Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.

Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Step 5 In the Group Notifications Settings section, for Email Updates, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **No email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Yes, send my updates to**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field.
- **On a schedule**—Click the radio button to choose this option and from the drop-down list, choose the how often you want to get updates from the Bug Toolkit.

Step 6 To save your changes, click **Save Search**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Note For complete Cisco Unified IP Phone firmware release note information, refer to the applicable firmware release notes for your specific IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/

Open Caveats

Table 7 describes possible unexpected behaviors in Cisco Unified Communications Manager Release 6.0(1), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 6 to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the “First Fixed-in Version” or “Integrated-in” fields. The information that displays in these fields 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.

- 005.000(000.123) = Cisco Unified Communications Manager Release 5.0(1)

- 005.000(001.008) = Cisco Unified Communications Manager Release 5.0(2)
- 005.001(002.201) = Cisco Unified Communications Manager Release 5.1(3)
- 006.000(000.123) = Cisco Unified Communications Manager Release 6.0(1)

Note Because defect status continually changes, be aware that Table 7 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "Using Bug Toolkit" section on page 111.

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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Table 7 Open Caveats as of 7/31/2007

Identifier	Headline
Component: Alarm Library	
CSCsj14755	After you insert a new server, change notification processing gets delayed.
CSCsj20653	Critical alarms occur when a large number of phones unregister simultaneously.
Component: Attendant Console	
CSCsj19702	Calls in a broadcast display as pilot points.
CSCsj86561	Attendant console displays "To Barge" in a shared line scenario.
CSCsj52448	A phone with extension mobility does not come up with Attendant Console.
CSCsj52461	Attendant Console displays "Conference to " when it is not appropriate.h
CSCsj52278	If you park a call on attendant console, "Parked Calls" displays the park information. If you log out and log back in to attendant Console, the park information in "Parked Calls" does not display.
CSCsj52327	On an attendant console in a shared line scenario, a call in the Remote-In-Use status can be parked.
CSCsj52411	Attendant Console does not open the dial windows when a shared phone gets reset.
CSCsj52428	User cannot switch between calls on attendant console.
CSCsj43140	Speed dial displays incorrect status for phone with 24 digit DN.
CSCsj70307	Speed dial DN status does not display correctly.
CSCsj43639	When a MeetMe call is transferred to attendant console, "Unknown to" displays.
CSCsj56483	User cannot place a new call in a shared line with Remote-In-Use.
CSCsj56416	User cannot perform a "First/Last Name" search in Advanced Directory.
CSCsj19756	When a called party parks a broadcast call and tries to retrieve it, the call does not display on the broadcast call list.
CSCsj19771	AC console displays Conference to XXX.

Table 7 Open Caveats as of 7/31/2007 (continued)

CSCsj19850	A transferred conference call gets displayed incorrectly in Cisco Unified Attendant Console.
Component: AXL	
CSCsi41224	The user cannot get the list of locales that are installed in the Cisco Unified Communications Manager by using thick AXL.
CSCsi55746	Enhancement: Update AXL:GetUser to indicate user license capabilities.
CSCsj78456	MOH server configuration fails.
Component: Bulk Administration Tool	
CSCsd55195	TAPS installation fails service won't start
Component: BPS-BAT	
CSCsi43409	BAT jobs remain in pending state.
Component: CAR	
CSCsi48348	When you try to open CDR analysis and reporting tool online help and the locale is Japanese, an HTTP 404 error is displayed.
Component: MIB Agent	
CSCsi85520	If the getbulk/getnext/getmany request contains multiple OID variables in its request PDU and the subsequent tables appear empty in the CISCO-CCM MIB, the responses may be NO_SUCH_NAME, for SNMP v1 version or GENERIC_ERROR, for SNMP v2c or v3 version because the time it takes to process the SNMP requests exceeds the MasterAgent timeout duration (currently set at 25 seconds).
Component: CLI	
CSCsi70101	You cannot stop or start platform agents by using the CLI or GUI.
CSCsh67199	You cannot configure ipadd on eth0 by using the **set network nic** CLI command.
CSCsj83200	The need exists for CLI commands to diagnose SNMP monitoring problems.
Component: Cisco Unified Communications Manager	
CSCsi94685	CTI: Some addresses do not have CallCtlAddrFwdEv Events.
CSCsi06589	CTI: Number of ConsultCalls does not get verified as in the range of the maximum consult calls.
CSCsj31611	Documentation: Disaster Recovery System documentation does not mention IP/hostname requirement.
CSCsj78966	Documentation:
CSCsj28919	UI: Script error displays when you navigate to the phone system menu in Cisco Unity Connection.
CSCsj54327	UI: English displays in Japanese Cisco Unified CM OS Administration windows.
CSCsj26028	UI: User cannot user BAT to delete unassigned DNs.
CSCsi62093	UI: Incorrect EVM-HD subunit number exists in Cisco Unified Communications Manager windows for SCCP analog gateways.
CSCsj64476	UI: The Firmware Load Information report incorrectly states that all 7914 modules are configured for non-default firmware.
Component: Call Processing	

Table 7 Open Caveats as of 7/31/2007 (continued)

CSCsj09704	Call Control: Some performance counters continue to increase in value with secured calls.
CSCsj75977	Call Control: When you transfer a call via a SIP trunk that has MTP enabled, one-way voice results.
CSCsj65704	Database: When extension mobility is enabled, dbProcs hangs and does not respond to TSP requests.
CSCsj42975	Database: The service URL on the extension mobility login profile gets overwritten by the URL of the phone.
CSCsj85891	H323: When a call is made across a QSIG ICT, the phone does not display the called party name.
CSCek47003	Media Control: Notify media about video reservation gets lost mid-call.
CSCsj65202	Media Control: Wrong iLBC-codec RSVP bandwidth exists for T1 CAS/PRI.
CSCsj42779	Media Control: SCCP/MGCP in iLBC region call over SIP trunk fails after holding for 15 seconds.
CSCsj73468	Media Control: No escalation for TB - CUPC and call fails on hold and resume.
CSCsj57448	Media Control: MOH/RESUME problem in the Cisco Unified Application Environment.
CSCsi06692	Media Control: CallAgent controlled T.38 faxes from a Cisco gateway controlled by Cisco Unified Communications Manager to third-party H323 gateway fail.
CSCsj39371	Media Control: After users resume a mutual hold on SIP phones over asymmetric trunk, there is no audio.
CSCsj55498	Media Control: Call failure seen on a delayed open logical message from the Music on Hold (MoH) server.
CSCsj56172	Media Control: DTMF does not get recognized by third-party voicemail system.
CSCsj44752	Media Control: Blind transfer of a call across ICT failed.
CSCsg29976	Media Control: Video RSVP call to Cisco Unified Presence Communicator end point requires three RSVP resources.
CSCsh59632	Media Control: Video escalation/de-escalation does not work in some cases.
CSCsi71598	Media Control: One hour into a meeting, MeetingPlace Express conference participants get removed from a meeting and receive a series of voice prompts.
CSCsj81992	MGCP: After the PRI endpoint is reset by using Cisco Unified Communications Manager Administration, the user cannot receive or make calls through the MGCP gateway.
CSCsj63670	Mobility: Dual mode phone line does not get registered initially with LineControl.
CSCsi48312	SCCP: Extension mobility phone displays ASCII line text label instead of unicode.
CSCsi86093	SCCP: Phone gets multiple intercom calls setup if they come in using MLPP.
CSCsh64270	SCCP: Missed calls do not display for conference calls.
CSCsi87804	SCCP: SCCP performance degradation occurs.
CSCsh06653	SCCP: A conference call that is initiated by a 24-digit DN displays To External instead of To Conference.

Table 7 Open Caveats as of 7/31/2007 (continued)

CSCsj12850	SIP Station: TNP Cisco Unified IP Phones that are running SIP do not register on subscriber after it is reset.
CSCsi99657	SIP Station: In extreme situations when phones fail over and fall back repeatedly, a memory leak may exist.
CSCsj36505	SIP Station: CANCEL message does not include TAG information in the To: header.
CSCsj51238	SIP Station: SIP phone fails to display alerting name when OVERLAP sending gets used.
CSCsj63680	SIP Station: SIP registration fails if the username is all numeric.
CSCsj64362	SIP Station: When SIP phones register, a 486 Busy Here response occurs.
CSCsj69298	SIP Station: The Cisco Unified Communications Manager service restarts unexpectedly.
CSCsj70293	SIP Station: SIP dual-mode phone does not register successfully after the first registration attempt.
CSCsj86404	SIP Station: SIP phone in partially registered state.
CSCsi80593	SIP Station: SIP SDI traces get turned on/off by "Enable Forward & Miscellaneous Trace" in the SDI 'Trace Configuration' window.These traces cannot be controlled from 'SIP call Processing' check-box</B>
CSCsi84052	SIP Station: Measured BHCC performance dropped.
CSCsj54212	SIP Trunk: Call over SIP trunks fail and this message displays: Firewall syslog message: Deny TCP (no connection) from [IP]/[Port] to [IP]/5060 flags PSH ACK on interface [Interface Name].
CSCsj76015	SIP Trunk: Wrong connected name and number display for the originator call after Call Forward No Reply.
CSCsj68682	SIP Trunk: Calls get dropped.
CSCsd88710	SS Dcallpark: BLF displays busy when directed callpark DN is released in a shared line scenario.
CSCsi89279	Supplementary Services: Call Forward All activation from a phone takes more than 4 seconds to propagate to the rest of the cluster nodes.
CSCsj41228	Supplementary Services: Call Pickup Notify can only display 22 characters.
CSCse82461	Supplementary Services: Call pickup notification gets sent to devices previously assigned to the callpickup group but currently not in the same partition as the callpickup group.
CSCsi32626	System: Calls get rejected due to throttling at a low call rate and not at a higher call rate.
CSCsd50352	System: If you reset a device pool or any other object that can trigger a large scale device reset takes a long time to complete. While devices are resetting, publisher node CPU usage very high.
CSCsi74060	System: Device reset speed is slower than previous releases, especially in large scale clusters.
CSCsh36576	System: If the "DSCP for Cisco Communications Manager to Device Interface" enterprise parameter is set higher than CS4 (the default equals CS3), the signaling packets from Cisco Unified Communications Manager get tagged with DSCP 000000 instead of the configured DSCP, such as DSCP CS5 101000.

Table 7 Open Caveats as of 7/31/2007 (continued)

CSCsj13749	System: During heavy call processing some calls may experience excessive delays in processing or may get unexpectedly dropped. The condition may also lead to excessive media cut through delays.
CSCsj79613	System: Alpha cored.
Component: CPI	
CSCsi91410	Appinstall: Not enough disk space exists in the common partition to perform upgrade.
CSCsj86736	Appinstall: Cisco Unified Communications Manager installation DVD will fail media check or the installation does not complete.
CSCsj15172	Appinstall: Third-party COP file can cause service parameter problems after installation.
CSCsi51295	Certificate Management: Tomcat web certificate regeneration fails.
CSCsi81184	DMA: DMA installation fails and displays: "Error 1720. There is a problem with this Windows Installer Package. A script required for this install to complete could not be run. Contact your support personnel or package vendor."
CSCsh05766	DMA: DMA backup status displays “Ready” after the backup.
CSCsd11449	Operating System: BIOS does not get upgraded during an upgrade.
CSCsh54360	Operating System: Cisco Unified Communications Manager indicates that “verifyNetwork = Failed during bootup”; however, services that require network functionality operate as designed.
CSCse71209	Operating System: Updated recommended hard drive firmware list with models that have been experiencing excessive SCSI command timeouts. When one of these drives is present, user will see a POST message recommending he upgrade the drive's firmware. Failure to upgrade may result in the bus down-shifting from Ultra 320 to Ultra 3. See the “Smart Array 6i Requires HD Firmware Update to Avoid POST Notification” section on page 13.
CSCsj58803	Operating System: HP NC-Series broadcom firmware updates available for supported NICs. See the “HP NC-Series Broadcom Firmware Updates Available for Supported NICs.” section on page 13.
CSCsj58962	Operating System: Updated recommended hard drive firmware list with models that have been experiencing excessive SCSI command timeouts. When one of these drives is present, user will see a POST message recommending he upgrade the drive's firmware. Failure to upgrade may result in the bus down-shifting from Ultra 320 to Ultra 3. See the “Smart Array 6i Requires HD Firmware Update to Avoid POST Notification” section on page 13.
CSCsj49225	Operating System: A fresh install of Cisco Unified CM on the subscriber server stops during NTP setup; or, for already installed Cisco Unified CM nodes, the subscriber fails to closely track the publisher time.
CSCsj76935	Operating System: On a kernel panic with netdump configured, a backtrace gets dumped to the system console for every process in the system. This takes about 10-20 minutes and during this time the system is down and not available.
CSCsi39214	Operating System: BIOS settings on 7816I3 server may not be correct to support hard disk.
CSCsi90211	Operating System: 7835I2 mirroring causes the window to freeze.
CSCsj67456	Operating System: Upgrade JRE to pick up DST changes for New Zealand.

Table 7 Open Caveats as of 7/31/2007 (continued)

CSCsj07745	Operating System: High CPU/IOWait exists during IPCC load test.
CSCsi80568	Operating System: Unexpected call failures detected while running under heavy load during scheduled trace collection.
CSCsi75567	Operating System:Server restarts itself randomly. See http://www.cisco.com/warp/public/770/fn62850.shtml
CSCsg46442	Operating System: Cimserver CPU pegging on 7815-I1/2
CSCse81663	Operating System: iLO firmware that is installed on MCS-7825-H1, MCS-7835-H1, and MCS-7845-H1 platforms might be older than version 1.82, which contains critical bug fixes and comprises the minimum version required.
CSCse72363	Operating System: Tomcat logging gets done through syslog daemon that is using local 6.
CSCse71295	Operating System: Cisco recommends Hewlett-Packard firmware to minimize potential for media errors on SCSI HD version.
CSCsi88423	Platform API: Tomcat becomes nonresponsive after cluster upgrade due to OutOfMemoryError.
CSCsi88504	Service Manager: Platform CLI command utils service cannot stop/start/restart Cisco Tomcat server.
CSCsh76059	Toolkit: After a DRS restore of a cluster, restored scheduled trace collection jobs fail.
CSCsj56802	UI: Publisher server becomes inaccessible via Cisco Unified Communications Manager Administration and the phones cannot use IP Phone Services.
Component: Database	
CSCsi17347	CoW-dbrep reset extremely slow for 40ms RTT.
CSCsj62945	After an upgrade, CAR scheduler is activated automatically, but on **Serviceabiliy** > **Trace** > **Configuration** window, the service is marked as Inactive.
CSCsg90581	Upgrade by using DMA fails.
CSCsj64692	After upgrade, the new network service displays as inactive
CSCsh31645	Database replication suspect. "utils dbreplication status" indicates that replication is suspect because publisher tables have different number of rows from subscriber tables.
CSCsi83076	DMA fails when back slash character is used in Informix password.
CSCsi84391	Unset service parameter value remains the same even when default changes.
CSCsi50840	Windows RTMT or SFTP cannot download Informix RIS traces.
CSCsi41491	RTMT reports that are created by Informix creates core files named af.xxxxxxx.
CSCsb71648	Migration takes over 15 hours.
CSCsi35186	Extension mobility logins fail with an Error 6 Database failure.
CSCsc74763	The platform CLI command "run sql" results in some procedures or functions becoming inaccessible by using the EXECUTE FUNCTION or EXECUTE PROCEDURE syntax.
CSCse06687	Installation fails with cm-dbms-install failure.
CSCsj13610	Cisco Unified Communications Manager performed a core dump after upgrade.
CSCsj21949	Database throughput and response time take longer than in previous releases.

Table 7 Open Caveats as of 7/31/2007 (continued)

Component: IMS	
CSCsj42979	Login failure logs in syslog do not contain source IP address.
Component: IPMA Service	
CSCsj16278	Assistant phone status does not get updated in call transfer.
Component: JTAPI SDK	
CSCsg03945	CiscoJTAPIClient-linux.bin fails to install.
CSCsg13302	Downgrade to JTAPI client does not work properly.
Component: Licensing	
CSCsh79182	In the License File Upload window, license files with mismatched MAC addresses get displayed in the existing license files drop-down list.
Component: RISDC	
CSCsi51814	RIS data collector performance counter CSV logs rotate faster than the configured maximum file size.
Component: Real Time Monitoring Tool	
CSCsi83330	The permissions for RTMT Alert Config and RTMT Profile access do not get properly enforced.
CSCsi80661	RTMT client encounters an error collecting one specific trace file and aborts trace collection.
CSCsj57895	Trace collection scheduler disappears and the trace collection stops.
CSCsj42329	When you choose unregistered SIP devices in the RTMT Device Search window, the window does not update correctly. Works correctly for other states such as Registered.
Component: SNMP Research Agents	
CSCsi81864	If you stop Cisco Tomcat, it still displays as running under some conditions.
CSCsj25434	On 4GB and 6GB servers the virtual memory gets reported wrong by Host Agent.
Component: TAPISDK	
CSCsi48954	Shared line gets extra CONFERENCED call state on manual conference.
CSCsg23468	The first playwave operation gets delayed by a few seconds before the destination receives it.
CSCsi34579	Park Number does not display in conference list when one party parks in conference call.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Unified Communications Manager Release 6.0(1) documentation suite was released.

Note Cisco Unified Communications Manager Release 6.0(1a) contains no additional documentation updates.

- Omissions, page 121

Omissions

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Communications Manager 6.0(1).

Multicast Music On Hold and Media Termination Points

The following restriction exists for multicast music on hold (MOH) when a media termination point (MTP) is invoked.

When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, the caller hears silence instead of music on hold.

To avoid this scenario, configure unicast MOH or Tone on Hold instead of multicast MOH.

Cisco Unified IP Phones Supporting Cisco Call Back with PLKs

The Cisco Call Back chapter of the *Cisco Unified Communications Features and Services Guide* omits the following information:

Many Cisco Unified IP Phone models support the Cisco Call Back feature by using programmable line key (PLK).

The following URL lists the phone documentation that is available for the various Cisco Unified IP Phone models:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Intercom Configuration

The Intercom chapter in the *Cisco Unified Communications Manager Features and Services Guide* omits the following steps that should be taken to successfully install the intercom feature.

Step 1 From Cisco Unified Communication Manager Administration, click **Call Routing > Intercom**.

a. Create the intercom partition.

Note When you add a new intercom partition, Cisco Unified Communications Manager automatically adds a new intercom calling search space that contains only the new partition. You can modify the new intercom calling search space later.

b. Create the intercom directory number.

Note Be aware that intercom partition and calling search space cannot be mixed with partition and calling search space for regular lines.

Step 2 Click **Device > Device Settings > Phone Button Template** and add the intercom line to an existing phone button template or create new template.

Note Be aware that the intercom line cannot be configured as the primary line.

Step 3 Click **Device -> Phone** and assign an intercom directory number to the intercom line.

Step 4 Configure the intercom directory number and set up intercom speed dial, if desired.

Note You can configure the intercom line with a predefined destination (speed dial) to allow fast access.

Where to Find More Information

- The Intercom chapter of the *Cisco Unified Communications Manager Features and Services Guide Release 6.0(1)*
- The Intercom Directory Number chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.0(1)*
- The Intercom Calling Search Space chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.0(1)*
- The Intercom Partition chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.0(1)*
- The Phone Button Template Configuration Settings chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.0(1)*

Extension Mobility Redundancy

The Extension Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide* omits the following statement:

For information on extension mobility redundancy, see the Cisco Unified Communications Manager Applications chapter of the latest *Cisco Unified Communications SRND* that is located at http://www.cisco.com/go/srnd.

Serviceability Reports

The following information on serviceability reports does not exist in the *Cisco Unified Serviceability Administration Guide*.

If your network uses Network Address Translation (NAT) and you are trying to access serviceability reports inside the NAT, enter the IP address for the private network that is associated with the NAT in the browser URL. If you are trying to access the reports outside the NAT, enter the public IP address, and NAT will accordingly translate/map to the private IP address. To access serviceability reports after you log in to Cisco Unified Serviceability, choose **Tools > Serviceability Reports Archive.**

CTI Monitored Lines

To calculate the number of CTI monitored lines in a system, use the following formula:

number of pilot point DNs + (number of clients open * number of directory numbers per phone) + (number of parked directory numbers * number of open clients) = CTI Monitored Lines

Call Throttling and the Code Yellow State

The *Cisco Unified Communications Manager Features and Services Guide* includes the following feature description, but it does not represent a new feature. The documentation unintentionally omitted the description until now.

Call throttling allows Cisco Unified Communications Manager to automatically throttle (deny) new call attempts when it determines that various factors, such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation, or other events, could result in a potential delay to dial tone (the interval users experience from going off hook until they receive dial tone).

This chapter provides the following information about call throttling:

- Introducing Call Throttling, page 123
- Troubleshooting Call Throttling, page 125
- Related Topics, page 125

Introducing Call Throttling

Call throttling occurs automatically when Cisco Unified Communications Manager determines such conditions to be present, and the system exits throttling automatically when such conditions are alleviated. You can configure the parameters that are associated with entering and exiting call throttling through several service parameters in Cisco Unified Communications Manager Administration (**System > Service Parameters**) although Cisco does not advise modification of these parameters unless

recommended by Cisco customer support. See Service Parameters Configuration in the *Cisco Unified Communications Manager Administration Guide* for information on accessing and configuring service parameters.

Cisco Unified Communications Manager uses the values that are specified in the call-throttling-related parameters to evaluate the possibility of a delay to dial tone and also to determine when conditions no longer necessitate call throttling. When throttling is necessary to prevent excessive delay to dial tone, Cisco Unified Communications Manager enters a Code Yellow state, and new call attempts are throttled (denied). You can disable call throttling via the System Throttle Sample Size service parameter, but Cisco does not recommend disabling call throttling. The following list defines several of the call throttling-related service parameters:

- Code Yellow Entry Latency defines the maximum allowable delay, in milliseconds, to handle SDL messages that are sent to Cisco Unified Communications Manager by the various devices in the system as well as the wealth of internal messages that are received and sent by Cisco Unified Communications Manager for various activities such as KeepAlives, change notification, and many more types of internal messaging. If the calculated average expected delay is more than the value that is specified in this service parameter, Cisco Unified Communications Manager enters a Code Yellow state to initiate call throttling and stops accepting new calls.
- Code Yellow Exit Latency Calculation determines the acceptable percentage of Code Yellow Entry Latency to specify exit criteria for leaving the Code Yellow state (Code Yellow exit latency) when Cisco Unified Communications Manager has initiated call throttling. The basis for the value that you specify in this parameter comprises a formula that uses the value in the Code Yellow Entry Latency parameter, which specifies the delay in milliseconds. To arrive at a percentage, use the following formula: Code Yellow Entry Latency value multiplied by the Code Yellow Exit Latency value. For example:

  Code Yellow Entry Latency service parameter value: 20 msec

  Code Yellow Exit Latency service parameter value: 40%

  Code Yellow Exit Latency value = 20 X 0.4 = 8 msec, which means Cisco Unified Communications Manager exits Code Yellow state if the calculated message latency drops to 8 msec or lower.

  To get out of the Code Yellow state, Cisco Unified Communications Manager ensures that the average expected delay is less than the value of the Code Yellow exit latency.
- Code Yellow Duration specifies the number of minutes that a Cisco Unified Communications Manager system can remain in a Code Yellow state (call throttling). If this duration is met and the system is still in Code Yellow state, Cisco Unified Communications Manager enters a Code Red state, which indicates that Cisco Unified Communications Manager has remained in a Code Yellow state for an extended period and cannot recover. When Cisco Unified Communications Manager enters a Code Red state, the Cisco CallManager service restarts, which also produces a memory dump that may be helpful for analyzing the failure.
- System Throttle Sample Size indicates the size of the sample, in seconds, that is used to calculate the average expected delay for Cisco Unified Communications Manager to handle an SDL message. For example, a sample size of 10 means that Cisco Unified Communications Manager must calculate a non-zero latency value for 10 consecutive seconds before it will calculate the average expected delay and compare it to the value in the CodeYellow Entry Latency parameter. You can disable call throttling via this parameter.

When delay to dial tone is calculated to be over the threshold that is configured in the call-throttling-related service parameters, Cisco Unified Communications Manager begins rejecting new calls. When call throttling is engaged, a user who attempts a new call will receive reorder tone and, depending on the phone model, may also receive a prompt on the phone display. Call throttling effectively avoids the problem in which a user tries to place a new call, but the length of delay between going off hook and receiving dial tone is excessive enough to cause a reaction in the user (such as

complaining to the system administrator or questioning whether the system is down or the phone is broken, for example). Cisco Unified Communications Manager uses a complex algorithm to constantly monitor the system to anticipate when such latency could occur.

When the delay to dial tone is within the guidelines of the call-throttling-related service parameters, Cisco Unified Communications Manager ceases throttling calls by exiting the Code Yellow state, and new calls events are again allowed.

Troubleshooting Call Throttling

CCM/SDI and SDL trace files record call throttling events and can provide useful information. Also, you generally will require performance monitoring data for debugging. The Cisco Communications Manager System Performance object (viewable in the Real-Time Monitoring Tool) includes a counter called ThrottlingSampleActivity, which indicates whether Cisco Unified Communications Manager has calculated a non-zero value for latency and helps you understand how busy the system is. Frequent non-zero values in this counter could indicate a potential overload condition on the system. To try to circumvent the possibility of a Code Yellow event, consider the possible causes of a system overload, such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation or other such events, and begin to investigate those possibilities.

Generally, repeated call throttling events require assistance from the Cisco Technical Assistance Center (TAC). TAC will likely request these trace files for closer examination.

Related Topics

- Service Parameters Configuration in the *Cisco Unified Communications Manager Administration Guide*

Call Throttling and Denial of Service (DOS) Attacks

Cisco Unified Communications Manager adds two new parameters to help prevent Denial of Service (DOS) attacks: SIP Station UDP Port Throttle Threshold and SIP Trunk UDP Port Throttle Threshold. These thresholds define the maximum incoming packets per second that Cisco Unified Communications Manager can receive from a single (unique) IP address that is directed at the UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold. Be aware that the enterprise parameter Denial-of-Service Protection Flag must be set to True for these parameter values to take effect. See "Throttling on SIP UDP Ports" section on page 137 below for more information.

Number of Login or Logout Operations that Cisco Extension Mobility Supports

The *Cisco Unified Communications Manager Features and Services Guide* omits the maximum number of login or logout operations that Cisco Extension Mobility supports for Cisco Unified Communications Manager Release 6.0(1). The correct guideline follows:

Cisco Extension Mobility supports a maximum of 250 login or logout operations per minute (or 15,000 operations per hour). Remember that these operations are sequential, not concurrent. (Some devices may support more login or logout operations per hour.)

Using the G.722 Codec

The *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* do not provide the following information on the G.722 codec.

Cisco Unified Communications Manager 6.0 supports the Advertise G.722 codec enterprise parameter, which determines whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified Communications Manager. Codec negotiation involves two steps. First, the phone must advertise the supported codec(s) to Cisco Unified Communications Manager (not all phones support the same set of codecs). Second, when Cisco Unified Communications Manager gets the list of supported codecs from all phones that are involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting. This parameter only applies to Cisco Unified IP Phones 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE. Valid values specify True (the specified Cisco Unified IP Phones advertise G.722 to Cisco Unified Communications Manager) or False (the specified Cisco Unified IP Phones do not advertise G.722 to Cisco Unified Communications Manager).

Note The default for the Advertise G.722 Codec enterprise parameter enables G.722 on all phones in the cluster. The default value of the phone configuration Advertise G.722 Codec Product-Specific parameter uses the value that the enterprise parameter setting specifies.

The Product-Specific Configuration area in the Phone Configuration window supports the parameter, Advertise G.722 Codec. Use this parameter to override the enterprise parameter on an individual phone basis.

Table 7 indicates how the phone responds to the configuration options.

Table 8 How Phone Responds to Configuration Settings

Enterprise Parameter Setting	Phone (Product-Specific) Parameter Setting	Phone Advertises G.722
Advertise G.722 Codec Enabled (True)	Use System Default	Yes
Advertise G.722 Codec Enabled (True)	Enabled	Yes
Advertise G.722 Codec Enabled (True)	Disabled	No
Advertise G.722 Codec Disabled (False)	Use System Default	No
Advertise G.722 Codec Disabled (False)	Enabled	Yes
Advertise G.722 Codec Disabled (False)	Disabled	No

Cisco Unified Communications Manager supports G.722, which is a wideband codec, as well as a propriety codec simply named Wideband. Both represent wideband codecs. Wideband codecs such as G.722 provide a superior voice experience because wideband frequency response is 200 Hz to 7 kHz compared to narrowband frequency response of 300 Hz to 3.4 kHz. At 64 kbps, the G.722 codec offers conferencing performance and good music quality.

When users use a headset that supports wideband, they experience improved audio sensitivity when the wideband setting on their phones is enabled (it is disabled by default). To access the wideband headset setting on the phone, users choose the **Settings** icon > **User Preferences** > **Audio Preferences** > **Wideband Headset**. Users should check with their system administrator to be sure their phone system is configured to use G.722 or wideband. If the system is not configured for a wideband codec, they may not detect any additional audio sensitivity, even when they are using a wideband headset.

The following Cisco Unified IP Phones (both SCCP and SIP protocols) support the wideband codec G.722 for use with a wideband headset:

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G

When you choose a G.711 or G.722 codec in Region Configuration, you are choosing the bandwidth utilization. Choosing either codec produces the same effect. When you choose either G.711 or G.722, these codecs disallow selecting codecs that have a payload greater than 64 kbps, such as the G.722 wideband codec and Advanced Audio Codec (ACC) (when ACC uses more than one channel).

If you choose a region that is lower than G.711 or G.722, the Advertise G.722 Codec enterprise parameter gets ignored because the system does not allow G.722, G.711, AAC, and wideband.

Tip Disregard the following statements in the System Level Configuration chapter in the *Cisco Unified Communications Manager System Guide* and in the Region Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*: "The default audio codec for all calls through Cisco Unified Communications Manager specifies G.711. If you do not plan to use any other audio codec, you do not need to use regions." Because G.711 and G.722 use the same bandwidth, the system may use G.722 unless you choose False for the Advertise G.722 Codec enterprise parameter.

For more information about the G.722 codec, see the "Disabling the Advertise G.722 Codec Enterprise Parameter When You Are Using System Features" section on page 11.

New Cisco Signaling Performance Object

The Performance Objects and Counters for the Cisco Unified Communications Manager Appendix chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide* does not include the following updated information on the Cisco Signaling Performance Object.

The Cisco Signaling Performance object provides call-signaling data on transport communications on Cisco Unified Communications Manager.

The UDPPacketsThrottled counter represents the total number of incoming UDP packets that were throttled (dropped) because they exceeded the threshold for the number of incoming packets per second that is allowed from a single IP address. Configure the threshold via the SIP Station UDP Port Throttle Threshold and SIP Trunk UDP Port Throttle Threshold service parameters in Cisco Unified Communications Manager Administration. This counter increments for every throttled UDP packet that was received since the last restart of the Cisco CallManager Service.

Modifying HostName/IP Address Creates Inaccessible RTMT Profiles

The *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* does not include the following information about the inaccessibility of RTMT profiles when you modify the Host Name/IP Address field in Server Configuration.

RTMT saves RTMT configuration profiles in the database based on the host name or IP Address that the administrator entered in the Server Configuration in Cisco Unified Communications Manager Administration.

When you modify the Host Name/IP Address field in Server Configuration, you cannot access the RTMT profiles for that server. This includes changing the entry in the Host Name/IP Address field from the hostname to the IP Address and vice versa. When you modify the Host Name/IP Address field, you will need to recreate the profile the next time that you log in to the server on RTMT.

Collecting Installation Logs with RTMT

The *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* does not contain the following procedure that describes how to collect installation and upgrade logs in trace and log central.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **System**.
  - In the tree hierarchy, double-click **Tools**.
  - Click the Trace & Log Central icon.
- Choose **System > Tools > Trace >Trace & Log Central**.

The Trace & Log Central window displays.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Install Logs**.

The Collect Install Logs wizard displays

Step 3 In the Select Servers Options box, specify from which server you would like to collect the install logs. To collect the install logs for a particular server, check the check box next to the server. To collect the install logs for all servers, check the Select All Servers check box.

Step 4 In the Download File Options, specify the directory where you want to download the log file. To specify the directory in which you want to download the log files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 5 Click **Finish**.

Replication Status on Database Summary in RTMT

The Working with Cisco Unified Communications Manager Monitoring chapter in the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* does not contain the updated information on predefined database object in Cisco Unified Communications Manager:

The database summary provides connection information for the server, such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, the number or replicates that have been created, and the status of the replication.

For more information see the "Number of Replicates Created and State of Replication" section on page 140.

Creating an RTMT User

Cisco Unified Communications Manager supports the creation of a RTMT user with restricted access to Cisco Unified Communications Manager Administration. You can create a user with a profile that is limited to Cisco Unified Communications Manager RTMT usage only. The user will have full access to RTMT but will not have permission to administer a Cisco Unified Communications Manager server.

You can create a RTMT user by adding a new application user and adding the user to the predefined Standard RealtimeAndTraceCollection group.

For additional information on adding users and user groups, refer the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

set network dhcp eth0 disable Command Parameters

The **set network dhcp eth0 disable** command now requires the following parameters:

- *ip*—The new static IP address
- *mask*—The new network mask
- *gateway ip*—The new gateway IP address

Errors

This section provides information about errors that are contained in the Cisco Unified Communications Manager Release 6.0(1) documentation.

Default Device Profile Information

The Default Device Profile Configuration chapter of the *Cisco Unified Communications Administration Guide* incorrectly states that the Default Device Profile can be configured to subscribe to services. Disregard the following text:

- The entire section entitled "Subscribing Services to a Default Device Profile."
- The introductory sentence in the "Configuring a New Device Profile" section that includes "subscribed IP phone services" as one of the configurable attributes of the default device profile.

Call Admission Control Bandwidth Example Correction

The Call Admission Control chapter of the *Cisco Unified Communications Manager System Guide* incorrectly describes the amount of bandwidth that is consumed in an example locations-type call admission control scenario.

Original explanation:

Cisco Unified Communications Manager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kbps of available bandwidth, that link can support one G.711 call at 80 kbps (in each direction), three G.723 or G.729 calls at 24 kbps each (in each direction), or two GSM calls at 29 kbps each (in each direction). If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone.

Correct explanation:

Cisco Unified Communications Manager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kbps of available bandwidth, that link can support two G.711 calls at 80 kbps each, six G.723 or G.729 calls at 24 kbps each, or five GSM calls at 29 kbps each. If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone

Barge and Security

The "Restrictions" section of the Barge and Privacy chapter in the *Cisco Unified Communications Manager Features and Services Guide* misstates the capabilities of encrypted phones to accept barge requests from unencrypted phones or from calls with a lower security level in Cisco Unified Communications Manager Release 6.0(1x).

The correct information follows:

Any phone can barge in to any existing call regardless of security level. An icon on the phone indicates the lowest security level of all participants:

- A shield icon represents the authenticated security level
- A lock icon represents the encrypted security level
- If no icon exists, that means that the call has no security level

Barge Visual Indicator

The Cisco Unified IP Phone Configuration chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly states that a spinning circle on the phone display indicates that a barge is taking place. Only an audible indicator occurs.

Barge with Shared Conference Bridge

The Barge and Privacy chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not correctly describe the process for configuration of the Barge with Shared Conference Bridge feature. The Standard User and Standard Feature softkey templates do not support cBarge, and cannot be modified. The following corrections apply to Table 9-3, Barge with Shared Conference Bridge (cBarge) Configuration Checklist.

Replace Step 1 with the following information:

To create a softkey template that includes cBarge, make a copy of the Standard Feature softkey template. Modify this user-named copy to add the Conference Barge (cBarge) softkey to the Selected Softkeys in the Remote in Use call state. See the "Adding Non-Standard Softkey Templates" section in the ”Device Configuration chapter of the *Cisco Unified Communications Manager Administration Guide* for more information on creating copies of standard softkey templates.

After Step 3, insert the following sentence:

Disable privacy on phones to allow cBarge.

Serviceability Administration

Understanding Hardware MIB Support

The *Cisco Unified Serviceability Administration Guide* does not contain correct information on vendor-specific MIBs in the Understanding Simple Network Management Protocol chapter. When working with SNMP, use the following information about vendor-specific MIBs.

Tip The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that are developed by the hardware vendors; for example, HP Systems Insight Manager (SIM), IBM Director Server+Console, and Dell Open Manage. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 8—Describes supported IBM MIBs
- Table 9—Describes supported HP MIBs
- Table 10—Describes supported Dell MIBs

Table 9 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data

Table 9 IBM MIBs (continued)

MIB	OID	Description
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 10 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

Table 11 Dell MIBs

MIB	OID	Description
Supported for browsing and system traps		
MIB-Dell-10892	1.3.6.1.4.1.674.10892.1	Provides hardware component assets/status/events
StorageManagement-MIB	1.3.6.1.4.1.674.10893.1	Provides disk/RAID asset data
MIB-Dell-CM	1.3.6.1.4.1.674.10899	Provides operating system, BIOS, firmware data

Configuring Alarms for Services

The following information on alarms for the Cisco Extension Mobility Application service, Cisco IP Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer Web Service does not exist in the *Cisco Unified Serviceability Administration Guide*.

For alarm generation, the Cisco Extension Mobility Application service, Cisco IP Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer Web Service use Cisco Tomcat. The system login alarm AuthenticationFailed also uses Cisco Tomcat. To generate alarms for these services, perform the following procedure.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Alarms > Configuration**.

Step 2 From the Server drop-down list box, choose the server for which you want to configure the alarm.

Step 3 From the Services Group drop-down list box, choose **Platform Services**.

Step 4 If you want to do so, you can apply the alarm configuration for the service to all nodes in the cluster by checking the **Apply to All Nodes** check box; that is, if your configuration supports clusters.

Step 5 From the Services drop-down list box, choose **Cisco Tomcat**.

Step 6 Enable the alarm(s) for the alarm destination(s) and the alarm event level, as described in the *Cisco Unified Serviceability Administration Guide*.

Tip The system sends the alarm if the configured alarm event level for the specific destination in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, which are higher severity levels, the system does not send the alarm to the corresponding location.

To access the alarm definitions for the Cisco Extension Mobility Application service, Cisco IP Manager Assistant service, Cisco Extension Mobility service, and the Cisco WebDialer Web Service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window, as described in the *Cisco Unified Serviceability Administration Guide*.

Step 7 To save your configuration, click the **Save** button.

Adding an Administrator User to Cisco Unity or Cisco Unity Connection

The Application User chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can use the Create Cisco Unity Application User link in the Related Links drop-down list box to create an application user voice mailbox in Cisco Unity or Cisco Unity Connection. You use this link to add an administrator user to Cisco Unity or Cisco Unity Connection.

1. Correct the Next Steps section in “Configuring an Application User” section to read as follows:

   Next Steps

If you want to associate devices with this application user, continue with the "Associating Devices to an Application User" procedure.

To manage credentials for this application user, continue with the "Managing Application User Credential Information" procedure.

To add this administrator user to Cisco Unity or Cisco Unity Connection, continue with the procedure in "Adding an Administrator User to Cisco Unity or Cisco Unity Connection" section on page 134.

2. Correct the section header "Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox" to "Adding an Administrator User to Cisco Unity of Cisco Unity Connection" and correct the content as follows:

Adding an Administrator User to Cisco Unity or Cisco Unity Connection

The Create Cisco Unity Application User link on the Application Configuration window allows you to add this user as an administrator user to Cisco Unity or Cisco Unity Connection. With this method, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration

Note Cisco does not support Cisco Unity on Cisco Unified Communications Manager Business Edition systems.

You can also use the import tool in Cisco Unity or Cisco Unity Connection to import application users as administrative users. To import users, refer to the Cisco Unity or Cisco Unity Connection documentation. (The system does not support the import feature for Cisco Unity Connection 1.1 or 1.2.)

The Create Cisco Unity User link displays only if the Cisco Unity administrator installed and configured the appropriate software. Refer to the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or the applicable Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection.

Before You Begin

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection. For Connection users, refer to the applicable *User Moves, Adds, and Changes Guide for Cisco Unity Connection.* For Cisco Unity users, refer to the *Cisco Unity System Administration Guide*.

Procedure

Step 1 Find the application user, as described in "Finding an Application User" section.

Step 2 From the Related Links drop-down list box, in the upper, right corner of the window, choose the Create Cisco Unity Application User link and click **Go**.

The Add Cisco Unity User dialog box displays.

Step 3 From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click **Next**.

Step 4 From the Application User Template drop-down list box, choose the template that you want to use.

Step 5 Click **Save**.

The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to Edit Cisco Unity User in the Application User Configuration window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Note When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified Communications Manager Application User, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration), First Name, Last Name, Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Administration or Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Note Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration at the Tools menu. For Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* for more information. For Cisco Unity, refer to the *Cisco Unity System Administration Guide*.

Number of Alphanumeric Characters Allowed in the Pickup Group Name Field

The *Cisco Unified Communications Manager Features and Services Guide* incorrectly states that you can enter up to 30 alphanumeric characters in the Pickup Group Name field in the Call Pickup Group Configuration window. The guide should state that you can enter up to 100 characters in the Pickup Group Name field.

Updates

This section provides information that has been updated since the release of the Cisco Unified Communications Manager Release 5.1(1b) documentation.

Cisco Extension Mobility Supplemental Information

Consider the following information as supplementary to the information that is provided in the Cisco Extension Mobility chapter of the *Cisco Unified Communications Manager Features and Services Guide*:

When you subscribe devices to the Extension Mobility IP Phone Service (**Device > Device Settings > Phone Services**), an error results if you click **Update Subscriptions** more than once. When you update many phones, it can take some time for the changes to propagate to all devices. You must click **Update Subscriptions** only once and wait for this propagation to complete.

Cisco Unified IP Phones Supporting Barge

Replace the following out-of-date statement in the Barge and Privacy chapter of the *Cisco Unified Communications Features and Services Guide*:

Original statement:

Some Cisco Unified IP Phones (such as Model 7940 and 7960) have the built-in conference bridge capability, which barge uses.

Updated information:

Most Cisco Unified IP Phones include the built-in conference bridge capability, which barge uses.

Cisco Unified IP Phones Supporting Cisco Call Back

The "Interactions and Restrictions" section in the Cisco Call Back chapter of the *Cisco Unified Communications Features and Services Guide* has not been updated with regard to the specific Cisco Unified Communications Manager IP Phones that support Cisco Call Back.

The following URL lists the phone documentation that is available for the various Cisco Unified IP Phones:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

To check which phones support Cisco Call Back, see the phone Administration Guide for the phone in question and refer to the Telephony Features for the Cisco Unified IP Phone table.

To check which phones also support Cisco Call Back with PLKs, see the Phone User Guide for the phone in question and refer to the “Understanding Feature Availability” section.

Extension Mobility Successful Authentication Cache

The Extension Mobility application maintains a cache of all logged on user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user gets validated with information from the cache. This means that, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords get recognized.

Software Conference Bridge Not Supported

The Configuring Secure Conference Resources chapter in the *Cisco Unified Communications Manager Security Guide* requires this addition: Due to the performance impact to Cisco Unified Communications Manager processing, secure conferencing does not get supported on software conference bridge.

Throttling on SIP UDP Ports

The SIP and Cisco Unified Communications Manager chapter in the *Cisco Unified Communications Manager System Guide* requires this update for SIP UDP port throttling.

SIP UDP port throttle thresholds help prevent Denial of Service (DOS) attacks from SIP trunks and SIP stations. When the incoming packet rate exceeds the configured threshold for a SIP station or SIP trunk UDP port, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

The SIP Service Parameters section of this chapter does not include the following new parameters for SIP UDP throttling.

SIP UDP Port Throttling Thresholds

These throttle thresholds apply only to SIP UDP ports and do not affect SIP TCP or TLS ports.

Table 12 describes the configurable threshold values:

Table 12 SIP UDP Port Throttling Thresholds

Type	Default Value	Range	Definition
SIP Station UDP Port Throttle Threshold	50	10-500	The SIP Station UDP Port Throttle Threshold parameter defines the maximum incoming packets per second that Cisco Unified Communications Manager can receive from a single (unique) IP address directed at the SIP station UDP port.
SIP Trunk UDP Port Throttle Threshold	200	10-500	The SIP Trunk UDP Port Throttle Threshold defines the maximum incoming packets per second that a SIP trunk can receive from a single (unique) IP address directed at the SIP trunk UDP port.

The Incoming Port description in Table 15-1 in the *Cisco Unified Communications Manager Security Guide* requires this addition for SIP UDP Port Throttling:

Tip If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Cisco Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to this parameter to take effect.

Deleting a Server

The *Cisco Unified Communications Manager Administration Guide* does not provide the error messages that display when you attempt to delete a server. For information on these error messages, see the "Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration" section on page 8.

Disregard the entire section, "Deleting a Server," in the System-Level Configuration Settings chapter in the *Cisco Unified Communications Manager System Guide*. Instead, consider the following information when you delete a server:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node. When you attempt to delete a node, Cisco Unified Communications Manager Administration displays the message that is described in the "Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration" section on page 8.
- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.

Do Not Disturb Feature Priority

On Cisco Unified IP Phones, the text message that indicates the Do Not Disturb (DND) feature is active takes priority over the text message that indicates the user has new voicemail messages, which allows the user to know when DND is active. However, the text message that indicates the Call Forward All feature is active has a higher priority than DND.

Security Icons and Encryption

This subsection of the "Restrictions" section in the Security Overview chapter in the *Cisco Unified Communications Manager Security Guide* requires this addition:

- If a call from an encrypted phone over a SIP trunk gets transferred back to an encrypted phone in its own cluster, the call does not get encrypted, and the lock icon does not display even though the encrypted phones exist in the same secure cluster.

Changes

This section contains changes that have occurred since the release of the Cisco Unified Communications Manager Release 6.0 documentation. These changes may not appear in the current documentation or the online help for the Cisco Unified Communications Manager application:

- Recommended Number of Devices in Device Pool, page 139

Recommended Number of Devices in Device Pool

The following information from the *Cisco Unified Communications Manager System Guide*, Redundancy chapter, needs clarification.

You associate devices with a Cisco Unified Communications Manager group by using device pools. You can assign each device to one device pool and associate each device pool with one Cisco Unified Communications Manager group. You can combine the groups and device pools in various ways to achieve the desired level of redundancy.

Note A server can be in a single device pool and can support up to 7500 devices (high-end servers only). See your Cisco representative for information on the types of servers that Cisco Unified Communications Manager supports.

Devices Associated with the Attendant Console Application User

The Cisco Unified Communications Manager Features and Services Guide incorrectly states that administrators who are configuring Cisco Unified Communications Manager Attendant Console must associate devices with the Cisco Unified Communications Manager Attendant Console **ac** application user, unless the administrators enable the superprovider feature.

The document should state that administrators must always enable the superprovider feature by associating the **ac** application user with the user group "Standard CTI Allow Control of All Devices" and must not associate any devices with the Cisco Unified Communications Manager Attendant Console **ac** application user.

Caution System instability can occur if you associate devices to the Cisco Unified Communications Manager Attendant Console application user.

During an upgrade from Cisco Unified Communications Manager Release 4.x, the system automatically converts the **ac** application user to a superprovider user and disassociates the devices that were previously associated to the application user.

To enable device security for the Cisco Unified Communications Manager Attendant Console, configure an ACDeviceAuthenticationUser application user and associate the attendant phones with that user.

Number of Replicates Created and State of Replication

The System Appendix chapter in the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* does not include the following updated information on the Number of Replicates Created and State of Replication object. The Number of Replicates Created and State of Replication object provides information about the replication state on the system. The following information describes the counters for the Number of Replicates Created and State of Replication Object.

- Replicate_State - This counter, which displays the state of replication, includes the following possible values:
  - 0—Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed.
  - 1—The system created replicates of some tables but not all tables. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure.
  - 2—Good Replication.
  - 3—Bad Replication. When the counter displays a value of 3, replication in the cluster is bad. It does not mean that replication failed on a particular node. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure.
  - 4—Replication setup did not succeed.
- Number of Replicates Created - This counter displays the number of replicates that were created by Informix for the DB tables. This counter displays information during Replication Setup.

Credential Policy Settings

Table 104-1, Credential Policy Configuration Settings, in the Credential Policy chapter of the *Cisco Unified Communications Manager Administration Guide* requires the following changes:

- Change 1-10 to 1-100 in the Description column for the Failed Logon/No Limit for Failed Logons field.
- Change 1-120 to 1-1440 in the Description column for the Lockout Duration/Administrator Must Unlock field.

Support for Certificates from External CAs

This section in the Security Overview chapter of the *Cisco Unified Communications Manager Security Guide* updates the existing sentence to include IPSec and Tomcat, as follows: Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for Communications Manager, CAPF, IPSec, and Tomcat.

CAPF System Interactions and Requirements

This section in the Using the Certificate Authority Proxy Function chapter of the *Cisco Unified Communications Manager Security Guide* requires this new item:

- If a secure phone gets moved to another cluster, the Cisco Unified Communications Manager will not trust the LSC certificate that the phone sends because it was issued by another CAPF whose certificate is not in the CTL file. To enable the secure phone to register, delete the existing CTL file by using the “Deleting the CTL File on the Cisco Unified IP Phone” procedure in the *Cisco Unified Communications Manager Security Guide*. You can then use the Upgrade/Install option to install a

new LSC certificate with the new CAPF and reset the phone for the new CTL file (or use the MIC). Use the Delete option in the CAPF section on the Phone Configuration window to delete the existing LSC before the phones are moved.

Cisco Unified Phone Application Suite

Note Phone Application Suite support is not available until the 8.3(2) phone load gets released.

The following information from the *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones chapter, changed.

To configure the Cisco Unified Phone Application Suite for phones, the administrator must configure the following items:

- Set the Phone Personalization enterprise parameter to Enabled (disabled by default).
- Use the following configuration windows that contain the Phone Personalization field: Phone Configuration and Common Phone Profile.
- Download the Cisco Unified Phone Application Suite application from Cisco.com and deploy it to the user desktops by using your corporate policies and procedures.

For more information, see the *Cisco Unified Phone Application Suite Installation and User Guide*.

Peer-to-Peer Image Distribution

Use the following information from the *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones chapter, to replace the first paragraph of the “Peer to Peer Image Distribution” section.

The Peer Firmware Sharing feature provides these advantages in high-speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized TFTP servers.
- Eliminates the need to manually control firmware upgrades.
- Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously.

In most conditions, the Peer Firmware Sharing feature optimizes firmware upgrades in branch deployment scenarios over bandwidth-limited WAN links.

When enabled, it allows the phone to discover like phones on the subnet that are requesting the files that make up the firmware image and to automatically assemble transfer hierarchies on a per-file basis. The individual files that make up the firmware image get retrieved from the TFTP server by only the root phone in the hierarchy and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections.

For more information, see the applicable Cisco Unified IP Phone administration guide.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

Find a current list of security advisories, security notices, and security responses for Cisco products at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Find information about how to subscribe to the PSIRT RSS feed at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.