Release Notes for Cisco Unified Communications Manager Release 6.1(3a)

February 12, 2009

Caution Be aware that you can not upgrade directly from Unified CM 6.1(3x) to Unified CM 7.0

See:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

This document contains information pertinent to Cisco Unified Communications Manager Release 6.1(3x).

Table 1 Delta Between Release Notes for Unified CM 6.1(3) and Release Notes for Unified CM 6.1(3a)

Additions and Changes
• Added the "Caveats Resolved in Unified CM Release 6.1(3a)" section on page 8
• Updated the "Open Caveat as of February 12, 2009" section on page 100
• Added the "Description for Phone Personalization Is Incorrect in Documentation" section on page 139

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the "Upgrading to Cisco Unified Communications Manager 6.1(3x)" section on page 4 for information about upgrading and the "Important Notes" section on page 7 for information about issues that may affect your system.

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

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

Note 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 "Before You Begin" section on page 4.

Contents

These release notes discuss the following topics:

Introduction

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

System Requirements

Server Support

Make sure that you install and configure Cisco Unified Communications Manager Release 6.1(3a) on a Cisco Media Convergence Server (MCS) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which servers support the Cisco Unified Communications Manager Release 6.1(3a), 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 Make sure that the matrix indicates that your server model supports Cisco Unified Communications Manager Release 6.1(3a).

Note Some servers that are listed in the compatibility matrix may require additional hardware support for Cisco Unified Communications Manager Release 6.1(3a). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the compatibility matrix. Cisco Unified Communications Manager requires a minimum of 2 GB of memory, 72 GB disk drive, and 2 GHz processor.

To see which MCS server is compatible with Cisco Unified Communications Manager Release 6.1(3a), refer to http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html.

To find which servers support the Cisco Unified Communications Manager Release 6.1(3a), 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

Uninterruptible Power Supply

Ensure that you connect each Cisco Unified Communications Manager node to an uninterruptible power supply (UPS) to provide backup power and protect your system.

Caution Failure to connect the Cisco Unified Communication Manager nodes to a UPS may result in damage to physical media and require a new installation of Cisco Unified Communications Manager.

Installation Notes

The following sections comprise installation notes for Unified CM 6.1(3x).

- Windows 2000 Users Must Download Windows Installer 3.0 Updates, page 3
- Do Not Install Unified CM in a Large Class A or Class B Subnet That Contains a Large Number of Devices, page 4

Windows 2000 Users Must Download Windows Installer 3.0 Updates

If you are running Windows 2000 on your workstation or server, you must download Windows Installer 3.0 updates to correctly install CTL Client plug-ins. You can obtain Windows Installer 3.0 at the following URL:

http://www.microsoft.com/downloads/details.aspx?familyid=5FBC5470-B259-4733-A914-A956122E08E8&displaylang=en

Note Windows 2000 comes with Windows Installer 2.0.

Procedure

Step 1 Windows Installer 3.0 requires validation. Validate your PC by following the instructions.

Step 2 Install Windows Installer 3.0.

Step 3 Reboot your machine, if necessary.

Step 4 Proceed with CTL Client plug-ins installation.

Do Not Install Unified CM in a Large Class A or Class B Subnet That Contains a Large Number of Devices

Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default).

When the ARP table gets full, Cisco Unified Communications Manager experiences difficulty communicating with endpoints and cannot add more phones.

Upgrading to Cisco Unified Communications Manager 6.1(3x)

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

Before You Begin

Before you upgrade the software version of Cisco Unified Communications Manager, verify your current software version.

To do that, open Cisco Unified Communications Manager Administration. The following information displays:

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

Upgrade Paths To Cisco Unified Communications Manager 6.1(3x)

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

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Caution Use the ISO files that are mentioned in the "Upgrading From Cisco Unified Communications Manager Release 6.1(1x) or higher to Release 6.1(3a) by Using the UCSInstall File" section on page 5 for upgrades from 6.1(1x) and higher.

Upgrading to Unified CM 6.1(3x) From Unified CM 4.x and 5.x

If you are upgrading from 4.1.3, 4.2.3, 4.3(2), 5.1.2, or 5.1.3, use the Product Upgrade Tool (PUT) or the PUT for registered customers only to obtain a media kit and license or purchase the upgrade from Cisco Sales.

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

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

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Upgrading From an Engineering Special

if you want to upgrade to Cisco Unified CM 6.1(3a) and you are currently running an Engineering Special (ES), contact TAC to obtain the fixes that are included in the ES that you currently use.

Upgrading From Cisco Unified Communications Manager Release 6.1(1x) or higher to Release 6.1(3a) by Using the UCSInstall File

Will get the new build number when available.

Because of its size, the UCSInstall iso file, UCOS_6.1.3.2000-1.sgn.iso, comprises two parts:

- UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part1of2
- UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part2of2

Procedure

Step 1 From www.cisco.com, download the two UCSInstall files.

Step 2 Execute one of the following commands to reunite the two parts of the file.

Note The 6.1.3.2000-1 build represents a non-bootable ISO that is only useful for upgrades. You cannot use it for new installations.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part1of2 UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part2of2 UCSInstall_UCOS_6.1.3.2000-1.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the command prompt (cmd.exe) to combine the two parts:

```
COPY /B UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part1of2+UCSInstall_UCOS_6.1.3.2000-1.sgn.iso_part2of2 UCSInstall_UCOS_6.1.3.2000-1.sgn.iso
```

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

66fd64c2799d14db456cf589f1ed55be UCSInstall_UCOS_6.1.3.2000-1.sgn.iso

Software Download URLs

You can access the latest software upgrades for Cisco Unified Communications Manager 6.1 on Cisco.com. Table 2 lists the URLs from which you download the software.

Table 2 Download URLs for Software Upgrades

Software	Download URL
Cisco Unified Communications Manager 6.1(3x)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-61
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 6.1 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 6.1 as part of Unified Communications System Release 6.1 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 6.1 as part of Unified Communications System Release 6.1 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 6.1(3x). 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 6.1(3x).

Caveats Resolved in Unified CM Release 6.1(3a)

The following information comprises unexpected behavior that is addressed by this Service Update of Cisco Unified Communications Manager.

Identifier: CSCsw93549

Component : phones

Headline : Error in IP phone rules file causes sidecar not to register to Unified CM.

Identifier: CSCsx35470

Component : call processing

Headline : SDL version change for Unified CM 613a.

Identifier: CSCsx16330

Component : cli

Headline : Nodatasync option on switchversion causes permanent data loss.

Identifier: CSCsw97038

Component : sip trunk

Headline : Unified CM sends incorrect codec in SDP of ACK for outgoing mobility call.

Identifier: CSCsw76629

Component : mobility

Headline : Third-party SIP endpoint fails to register with digest authentication enabled.

SDI Trace Delete from User Interface May Cause High IO

This caveat is resolved in Unified CM 6.1(2), but not in 6.1(3x).

In Unified CM 6.1(3x), when you change the number of SDI trace files, all existing trace files get deleted. If the number of trace files is extremely large, this can cause high IOWait problems and phones may unregister.

Workaround

Manually delete the excessive trace files during off hours.

Use the CLI to delete the files first and then use the Trace Configuration window to update the maximum number of files or the maximum file size settings.

Cisco recommends that you delete the files in batches of 500 files, or fewer, at a time.

Example

Since CLI support “wild card” characters, to delete trace files from ccm00000600.txt to ccm00000699.txt use following CLI:

file delete activelog cm/trace/ccm/sdi/ccm000006*.* noconfirm

The CLI command does not delete files that are currently open, so there will not be any interruption to the current ccm trace log.

Ensure that files that you intend to delete are of no value; otherwise, download them before deleting them.

Cisco Unified JTAPI

In Cisco Unified Communications Manager Releases 6.x and 5.x, if an application tries to conference two or more addresses on the same terminal, based on the order of participants in the request, an application may receive CiscoJtapiException.CONFERENCE_INVALID_PARTICIPANT for the conference request. The conference might then start successfully with some of the participants. In such cases, no guarantees exist which application joins the conference. The system creates the conference with only one of the addresses on a terminal. It ignores the other addresses.

This situation occurs in the following scenarios.

Scenario 1

Assume that B1 and B2 represent different addresses on the same terminal, TB.

A -> B1 – GC1

A -> B2 – GC2

A -> C – GC3

Assume that an application issues a conference request GC1.conference(GC2,GC3).

In Cisco Unified Communications Manager Releases 6.x and 5.x, the application receives CiscoJtapiException.CONFERENCE_INVALID_PARTICIPANT; however, A, B1, and C join into conference, and the following normal set of events in a conference scenario occur:

```
GC1 CiscoConferenceStartEv

GC2 TermConnDroppedEv TB
GC2 CallCtlTermConnDroppedEv TB
GC2 ConnDisconnectedEv B1
```

```
GC2 CallCtlConnDisconnectedEv B1
GC1 CallCtlTermConnTalkingEv TB
GC2 CiscoCallChangedEv

GC1 ConnCreatedEv C
GC1 ConnConnectedEv C
GC1 CallCtlConnEstablishedEv C
GC1 TermConnCreatedEv TC
GC1 TermConnActiveEv TC
GC1 CallCtlTermConnTalkingEv TC

GC2 TermConnDroppedEv TC
GC2 CallCtlTermConnDroppedEv TC
GC2 ConnDisconnectedEv C
GC2 CallCtlConnDisconnectedEv C
GC2 CallInvalidEv
GC1 CiscoConferenceEndEv
```

Scenario 2

Assume that B1 and B2 represent different addresses on the same terminal, TB.

A -> B1 – GC1

A -> B2 – GC2

A -> C – GC3

Assume that an application issues a conference request GC3.conference(GC1,GC2).

In Cisco Unified Communications Manager Releases 5.x, the application does not receive an exception, and the request processes successfully. A, C, and B1 join the conference with the regular set of conference events.

In Cisco Unified Communications Manager releases 5.x 6.x, the application receives CiscoJtapiException.CONFERENCE_INVALID_PARTICIPANT; however, A, C, B1 join conference, and the normal set of conference events occurs.

SFTP Server Products

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

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

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

Cisco CallManager Service Stops After Upgrade to Cisco Unified Communications Manager 6.x

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

Immediately after you complete the upgrade, upload the software feature license that is required for Cisco Unified Communications Manager 6.X in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager.

For more information on licensing, refer to the licensing chapters in the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Important Information About Delete Transaction Using Custom File in BAT

Do not use the insert or export transaction files that are created with bat.xlt for the delete transaction. Instead, you must create a custom file with the details of the records that need to be deleted. Use only this file for the delete transaction. In this custom delete file, you do not need a header, and you can enter values for name, description, or user.

Partition Size Limitations When You Upgrade From a 5.x Release to a 6.x Release

Cisco Unified Communications Manager 5.x releases create disk partitions of a fixed size. If you install a 5.x release on a server with more disk space than required by the fixed partitions, the partitions still get created at the fixed size.

When you upgrade such a server from a 5.x release to a 6.x release, the disk partitions remain at the fixed size. If you perform a fresh installation of a 6.x release, the disk partitions get created as percentages of the available disk space, so your server will use all the available disk space effectively.

Cisco Unified Communications Manager Does Not Support Recovery of Administration or Security Passwords

Cisco Unified Communications Manager does not support recovery of administration or security passwords. If you lose these passwords, you must reset the passwords, as described in the *Cisco Unified Communications Operating System Administration Guide*.

The *Cisco Unified Communications Operating System Administration Guide* calls the section "Recovering the Administrator or Security Passwords" instead of "Resetting the Administrator or Security Passwords." Access the "Recovering the Administrator or Security Passwords" section to reset the passwords.

Deleting a Server and Adding a Deleted Server to a Cluster

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 CM 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 CM database and is not available for use.

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

Before you delete a server, consider the following information:

- Cisco Unified CM Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.
- Cisco recommends that you do not delete any node that has Cisco Unified CM 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 CM 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 CM Administration.
- If a configuration field in Cisco Unified CM Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.
- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or hostname for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.
- 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.
- Changes to the server configuration do not take effect until you restart Cisco Unified CM. For information about restarting the Cisco CallManager service, refer to the serviceability documentation for Cisco Unified CM.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server.
- After you delete the node, access Cisco Unified Reporting to verify Cisco Unified CM removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

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

Procedure

Step 1 In Cisco Unified CM Administration, add the server by choosing System > Server.

Step 2 After you add the subsequent node to Cisco Unified CM Administration, perform an installation on the server by using the disk that Cisco provided in your software kit.

Tip For example, if you have a version 6.1(3x) disk, perform a 6.1(3x) installation on the node. If you have a disk with a compatible version of 5.X on it, for example, use the disk to install Cisco Unified CM on the subsequent node; during the installation, choose the **Upgrade During Install** option when the installation displays the options.

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 Cisco Unified Communications Manager 6.1(3x) version 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 toinstallation documentation that supports your version of Cisco Unified CM.

Step 3 After you install Cisco Unified CM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco Unified CM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Clarification for Call Park Configuration

Consider the following information when you configure Call Park:

Call Park numbers cannot overlap between Cisco Unified CM servers. Ensure that each Cisco Unified CM server has its own unique number range.

Call Park numbers may have an associated partition that restricts access to the Call Park numbers and prevents retrieval of parked calls. If partitions are used to restrict access to Call Park numbers, you must define a unique call park number or range of call park extension numbers for each partition on each Cisco Unified Communications Manager in the cluster.

When the end user invokes Call Park, Cisco Unified Communications Manager attempts to find an available Call Park number from a Call Park partition that is currently accessible via the calling search space for the party that invoked Call Park.

Viewing Privileges for Roles in Cisco Unified CM Administration

The Role Configuration window in Cisco Unified CM Administration displays the privileges for each standard role. To access the Role Configuration window, find the role by choosing **User Management > Role**; when the Find and List Roles window displays, click **Find**. Click the link for the standard role that you want to view. After the Role Configuration window displays, you can view the privileges in the Resource Access Information pane.

TAPS Name Change in Bulk Administration Tool

Documentation refers to the Tool for Auto-Registered Phone Support (TAPS) as Cisco Unified Communications Manager Auto-Register Phone Tool in the Online Help for Bulk Administration. All references to 'Cisco Unified Communications Manager Auto-Register Phone Tool' in the Bulk Administration Tool Online Help should be read as 'Tool for Auto-Registered Phone Support (TAPS)'. This makes the terminology compliant with the Bulk Administration user interface.

For More Information

For information on configuring additional features in BAT, refer to the BAT documentation for Cisco Unified CM.

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

Alternatively, on MCS-7835H2, you can execute the **show ups** CLI command that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started.

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

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

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

CSCsq22385 Database Replication Setup Fails After You Add a New Subscriber to a Cluster

Database replication failure alert displays after you add a new subscriber node to an existing cluster. After the fresh install completes successfully, the following alert displays (date and time vary).

```
May 7 16:02:09 lg-pub-1 local7 2 : 116: May 07 20:02:09.491 UTC :
%CCM_RTMT-RTMT-2-RTMT-ERROR-ALERT: RTMT Alert Name:DBReplicationFailure Detail:
DBReplicationFailure occured. CallManager database replication errors, Reason code:
Replication setup failed. The alert is generated on Wed May 07 16:02:09 EDT 2008 on node
10.1.1.1. App ID:Cisco AMC Service Cluster ID: Node ID:xxx
```

The primary AMC server, which by default represents the publisher node, raises the DBReplicationFailure alert. You can observe this alert by using RTMT Alert Central or Summary view. You can also find the alerts in the EventViewer - Application Logs (CiscoSyslog) that you can access by using RTMT syslog viewer or platform CLI by using the **file view activelog syslog/CiscoSyslog** command.

Other Symptoms

The following list gives more symptoms of DBReplicationFailure that you may experience:

1. In the database replicator traces that are available on the publisher node. you may see the following error when you attempt to get the subscriber DB replication set up.

   ```
   dbl_repl_cdr_define_lg_sub_8_ccm6_1_2_1000_13-2008_05_07_12_00_20.log

   sucmd_err [su -c 'ulimit -c 0;cdr err --zap' - informix ]
   Executing [su -c 'ulimit -c 0;cdr define server --connect=lg_sub_8_ccm6_1_2_1000_13
   --idle=0 --init --sync=g_lg_pub_1_ccm6_1_2_1000_13 g_lg_sub_8_ccm6_1_2_1000_13
   --ats=/var/log/active/cm/log/informix/ats --ris=/var/log/active/cm/log/informix/ris;'
   - informix]
   We got exception in Cdr define
   Exception from cdr define e.value[100] e.msg [Error executing [su -c 'ulimit -c 0;cdr
   define server --connect=lg_sub_8_ccm6_1_2_1000_13 --idle=0 --init
   --sync=g_lg_pub_1_ccm6_1_2_1000_13 g_lg_sub_8_ccm6_1_2_1000_13
   --ats=/var/log/active/cm/log/informix/ats --ris=/var/log/active/cm/log/informix/ris;'
   - informix] returned [25600]]
   ```

2. The subscriber node Cisco DB logs (ccm.log) may include the following error:

   ```
   11:47:51 CDR GC: GC could not verify the local server identity in CDR catalog with
   that in sqlhost file during CDR recovery.
   ```

3. You cannot register any devices on the newly installed subscriber node because replication is not set up to the node.

By default, the publisher node DB replicator service continuously attempts to define the new server and generates a new log every 5 minutes.

Workaround for a Single Node

Use the following workaround for this caveat.

Caution Before you continue, identify the exact subscriber that is affected. To do that, look at the alert and confirm the node (IP) and the Node ID (hostname). In the preceding example alert, that information includes

```
node 10.1.1.1. App ID:Cisco AMC Service Cluster ID: Node ID:xxx
```

Step 1 Confirm that the reason for the DB replication failure is **cdr define** failure and then perform Step 2.

Step 2 From the platform CLI on the subscriber server, enter the following command:

utils dbreplication stop.

Caution This process can take 5 minutes or more to complete.

Wait for it to finish before you continue.

Step 3 From the platform CLI on the subscriber server, enter the following command:

utils dbreplication dropadmindb

Step 4 From the platform CLI on the publisher server, enter the following command.

utils dbreplication reset <*subname*> (<*subname*> equals the name of the subscriber server)

At the end of the command output, the following message displays:

```
admin:utils dbreplication reset nw104a-195
Repairing of replication is in progress.
Background repair of replication will continue after that for 30 minutes..
command failed -- Enterprise Replication not active  (62)
```

This output does **not** indicate a failure in the reset command. It serves as an informational message that got generated when you dropped the admindb on the subcriber server. The reset will complete successfully.

The reset command returns immediately, but the operation can take 30 minutes or more to finish.

Workaround for Multiple Nodes

The preceding instructions apply for single nodes, but multiple subscriber servers may experience this failure. If that occurs, for each subscriber node that is a fresh install and displays the DBReplicationFailure alert, repeat the preceding steps.

Verification

Be aware that replication is set correctly when the RTMT Replication counter "Replicate_State" equals 2 for both the publisher server and the subscriber server that you reset.

You can monitor the counter via the RTMT Database Summary window or via the platform CLI.

Strict Version Checking

Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.

Note Make sure that the restore runs on the same Cisco Unified Communications Manager version as the backup. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore.

Consider the following examples of restore to understand strict version checking:

Table 3 Restore Examples

From version	To version	Allowed / Not allowed
6.1.(1).1000-1	6.1(2).1000-1	Not allowed
6.1.(2).1000-1	6.1(2).1000-2	Not allowed
6.1.(2).1000-1	6.1(2).2000-1	Not allowed
6.1.(2).1000-1	6.1(2).1000-1	Allowed

In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unified Communications Manager database restore.

Serviceability Not Always Accessible from OS Administration

In some scenarios, you cannot access Cisco Unified Serviceability from Cisco Unified OS Administration. The window displays a "Loading, please wait" message indefinitely.

If the redirect fails, log out from Cisco Unified OS Administration, select Cisco Unified Serviceability from the navigation menu, and log in to Cisco Unified Serviceability.

Voice Mailbox Mask Interacts with Diversion Header

When a call gets redirected from a DN to a voice-messaging server/service that is integrated with Unified CM by using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. Be aware that this behavior is expected because the Unified CM server uses the diversion header to choose a mailbox.

CTL Client 5.0 Plug-In Installation Note

If you are upgrading to the CTL Client 5.0 plug-in, you first need to remove eToken Run Time Environment 3.00 by performing the following steps:

Procedure

Step 1 Download Windows Installer Cleanup Utility at the following URL:

http://support.microsoft.com/kb/290301

Step 2 Install the utility on your PC.

Step 3 Run the utility.

Step 4 Find eToken rte3.0 in the list of programs and remove it.

Step 5 Proceed with CTL Client installation.

Out-of-Service Nodes and Cisco License Manager

Symptom

After an upgrade from Cisco Unified CallManager Release 5.1(x) to Cisco Unified Communications Manager 6.1(3x), apply the 6.x software license. Restart Unified CM services on all nodes. Cisco Unified Communications Manager and all services start, except Cisco License Manager. Attempts to manually restart Cisco License Manager do not succeed.

Workaround

If dummy nodes exist in the cluster, you should map the IP addresses of the dummy nodes to the hostnames in the DNS server. If you do not, Cisco Unified Communications Manager generates alarms to indicate that the License Manager service is down.

Reset the Cluster After You Change the Security Password

Servers in a cluster use the Security password to authenticate communication between servers.

To change the Security password, use the **set password security** CLI command or reset the password from the console.

Step 1 Change the security password on the publisher server (first node) and then reboot the server (node).

Step 2 Change the security password on all the subsequent servers/nodes to the password that was created in Step 1 and restart subsequent nodes, including application servers, to propagate the password change.

Note Cisco recommends that you restart each server after the password gets changed on that server.

Note Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

Best Practices for Assigning Roles to Serviceability Administrators

Cisco recommends that you configure application users, rather than end users, to access remote nodes to perform such tasks as starting and stopping services. Starting and stopping services requires that the Standard Serviceability Administration and Standard RealtimeAndTraceCollection roles be assigned.

For Serviceability, the Administrator That Is Created During Installation Must Not Be Removed

Removing the Administrator that is created during installation or upgrade can cause communication with remote nodes via Serviceability Administration to fail.

Connecting to Third-Party Voice Messaging Systems

Administrators can connect third-party voice-messaging systems to Cisco Unified Communications Manager. Ensure the voice-messaging system has a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager Release 5.0 or later, use a Cisco certified serial-to-USB adapter with the part number USB-SERIAL-CA=.

Database Replication When You Revert to an Older Product Release

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

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

For information about the utils dbreplication clusterreset, utils dbreplication dropadmindb, and utils dbreplication forcedatasyncsub commands, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 7.0(1) document at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/7_0_1/cli_ref.html.

User Account Control Pop-up Window Displays During Installation of RTMT

When you install RTMT on the Microsoft Vista platform, the system displays the User Account Control pop-up window to indicate that an unidentified program wants access to your computer. This occurs because of a limitation in the InstallAnywhere software. This one-time pop-up displays only when you are installing RTMT. To continue, select **Allow**.

CiscoTSP Limitations on Windows Vista Platform

Always perform the first-time installation of the CiscoTSP and Cisco Unified Communications Manager TSP Wave Driver on a Vista machine as a fresh install.

If secure connection to Cisco Unified Communications Manager is to be used, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for inbound audio streaming, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for audio streaming, disable all other devices in the "Sound, video and game controllers" group.

Time Required for Disk Mirroring

Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.

Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 hours.

Cisco Unified Mobility Supports Nine Locales

Cisco Unified Mobility (Mobile Connect and Mobile Voice Access) support a maximum of nine locales, so Cisco Unified Communications Manager Administration blocks you from configuring 10 or more locales for Cisco Unified Mobility. In the Mobility Configuration window, more than nine locales can display in the Available Locales pane if they are installed for Cisco Unified Communications Manager, but you can only save nine locales in the Selected Locales pane. If you attempt to configure more than nine locales for Cisco Unified Mobility, the following message displays: "Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed."

Each Remote Destination Supports a Maximum of Two Active Calls

For Cisco Unified Mobility, each remote destination supports a maximum of two active calls via Cisco Unified Communications Manager. Using the enterprise feature access directory number (DID number) to transfer or conference with DTMF counts as one call. When a Cisco Unified Mobility user receives a call while the user has two active calls for the remote destination or while the user is using DTMF to transfer/conference a call from the remote destination, the received call does not reach the remote destination and instead goes to the enterprise voice mail; that is, if Call Forward No Answer (CFNA) is configured or if the call is not answered on a shared line.

Changes to Cisco Extension Mobility After Upgrade

If you chose a user-created profile from the Log Out Profile drop-down list on the Phone Configuration window and checked the Enable Extension Mobility check box, the settings in that profile become the permanent settings on the phone after an upgrade from Cisco Unified CallManager 4.x or Cisco Unified Communications Manager 5.x to Cisco Unified Communications Manager 6.1(1a).

RTMT Requirement When Cisco Unified Communications Manager Is Upgraded

If you are running the Cisco Unified Communications Real-Time Monitoring Tool (RTMT) client and monitoring performance counters during a Cisco Unified Communications Manager upgrade, the performance counters will not update during and after the upgrade. To continue monitoring performance counters accurately after the upgrade completes, you must either reload the RTMT profile or restart the RTMT client.

Serviceability Session Timeout Not Graceful

When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before it indicates that the session timed out and redirects you to the login window. After you log in again, you may need to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows.

Workaround

If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Problem Configuring Mobility Identity for Nokia S60 Device in Cisco Unified Communications Manager Administration

The following message may display in the Phone Configuration window in Cisco Unified Communications Manager Administration when you try to configure Mobility Identity for the Nokia S60 device: "Add failed. [10102] Check the type of device specified in fkDevice_DualMode. Remote Destionations other than Dual Mode must use fkDevice_RemoteDestinationTemplate."

The error occurs under one of the following circumstances:

- Circumstance 1—You provisioned Nokia S60 devices by using the pre-6.1(1a) Nokia S60 .cop file before or after you upgraded to Cisco Unified Communications Manager 6.1(1a). After you installed the latest 6.1(1a) compatible Nokia S60 .cop file, you tried to configure Mobility Identity for an existing Nokia S60 device in the Phone Configuration window in Cisco Unified Communications Manager Administration.
- Circumstance 2—Previously, you provisioned Nokia S60 devices by using the pre-6.1(1a) Nokia S60 .cop file. Then, you installed the latest 6.1(1a) compatible Nokia S60 .cop file. After the latest .cop file was installed, you tried to configure Mobility Identity for an existing Nokia S60 device in the Phone Configuration window in Cisco Unified Communications Manager Administration.

If the message displays, you can perform the following tasks to ensure that you can configure Mobility Identity for the Nokia S60 device:

1. In Cisco Unified Communications Manager Administration 6.1, disable auto-registration.
2. In the Find/List Phone window in Cisco Unified Communications Manager Administration, delete all Nokia S60 records.

Tip In case of large number of existing Nokia devices, Cisco recommends that you delete the Nokia S60 records by using the Bulk Administration Tool by choosing **Bulk Administration > Phones > Delete Phones**

3. In Cisco Unified Communications Manager Administration, configure all Nokia S60 devices by choosing **Device > Phone > Add New > Nokia S60**.

Tip For a large number of Nokia S60 devices, you can provision the devices in the Bulk Administration Tool by choosing **Bulk Administration > Phones > Insert Phones**.

4. Reset all Nokia S60 devices.

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

Table 4 lists the locations where you can configure a host name for the Cisco Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Cisco Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Caution Before you change the host name or IP address for any locations that are listed in Table 4, refer to *Changing the IP Address and Host Name for Cisco Unified Communications Manager 5.x and 6.x Servers* . Failing to update the host name or IP address correctly after it is configured may cause problems for Cisco Unified Communications Manager.

Table 4 Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System > Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for any server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation	You can add the host name for any server in the cluster.	1-63	alphabetic	alphanumeric
Hostname field **Settings > IP > Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric
set network hostname *hostname* Command Line Interface	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric

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

Before you configure the host name in any of the locations in Table 4, review the following information:

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

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

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

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

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

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

Related Topics

- "Server Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*
- *Installing Cisco Unified Communications Manager, Release 6.1(1)*
- *Cisco Unified Communications Operating System Administration Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions*
- *Changing the IP Address and Host Name for Cisco Unified Communications Manager 5.x and 6.x Servers*

Serviceability Limitations When You Modify the IP Address

When you modify the IP Address field, you cannot access the RTMT profiles, custom counters, custom alerts, and generic queries for Trace & Log Collection Tool (TLC) for that server.

You should manually remove any RTMT profiles, custom counters, custom alerts, and generic queries for Trace and Log Collection Tool (TLC) that were set for the old IP Address. When you modify the IP Address field, you will need to re-create the RTMT profile, custom counters, custom alerts, and generic queries for TLC the next time that you log in to the server on RTMT.

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

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

SIP Network/IP Address Field Required for SIP Fallback to SRST Gateway

Although Cisco Unified Communications Manager Administration does not list the SIP Network/IP Address field as a required setting, you must configure the SIP Network/IP Address field and the SIP Port field in the SRST Reference Configuration window for a SIP device to fall back to the SRST-enabled gateway. For more information on these fields and SRST references, refer to the *Cisco Unified Communications Manager Administration Guide*.

Online Help Was Not Updated for Cisco Unified Communications Manager, Release 6.1(3x)

When you view online help in Cisco Unified Communications Manager 6.1(3x), be aware that the online help did not get updated for 6.1(3x). The following graphical user interfaces (GUIs) contain online help:

- Cisco Unified Communications Manager Administration, which displays online help from 6.1(1)
- Cisco Unified Reporting, which displays online help from 6.1(1)
- Cisco Unified Serviceability, which displays online help from 6.1(1)
- Cisco Unified Communications Operating System Administration, which displays online help from 6.1(1)

For information on features that were introduced in Cisco Unified Communications Manager 6.1(2), refer to the *Release Notes for Cisco Unified Communications Manager Release 6.1(2)*. For a list of documents that were updated for Cisco Unified Communications Manager 6.1(2), refer to the *Cisco Unified Communications Manager Documentation Guide for Release 6.1(2)*.

New and Changed Information in Cisco Unified Communications Manager 6.1(3x)

The following section describes new features and changes that are pertinent to Cisco Unified Communications Manager, Release 6.1(3x) or later. The sections may include configuration tips for the administrator, information about users, and information about where to find more information.

Installation, Upgrade, and Migration

The following sections describe the changes for installation, upgrade, and migration in Cisco Unified Communications Manager 6.1(3x):

Cisco Security Agent for Cisco Unified Communications Manager Log File

The CLI command that accesses the Cisco Security Agent file log changed to **utils create report csa**.

System History Log for Cisco Unified Communications Manager

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

Description

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

Overview

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

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success and failure or cancellation of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.
- Logs every invocation of Switch Version that is issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown that is issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot results from a manual reboot, power cycle, or kernal panic.
- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. Access the log from the CLI by using the **file** commands and by using the Real Time Monitoring Tool (RTMT).

System History Log Fields

Each system history log entry contains the following fields:

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

The log also displays a common header which contains information about product name, product version and kernel image.

```
========================================
Product Name -    Cisco Unified Communications Manager
Product Version - 7.1.0.39000-9023
Kernel Image -    2.6.9-67.EL
========================================
```

The system history log fields can contain the following values:

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

Example

Example 1 shows a sample of the system history log.

Example 1 System History Log

```
admin:file dump install system-history.log
```

```
======================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
======================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 14:50:38 | root: Boot 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start
07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success
07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

CLI Considerations

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

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

Cisco Unified Communications Manager Administration Configuration Tips

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

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

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

Installation/Upgrade (Migration) Considerations

No installation or upgrade consideration exist for this feature.

Serviceability Considerations

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

RTMT > Trace Log Collection

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

For More Information

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

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

Data Migration Assistant (DMA) Enhancements

Cisco Unified Communications Manager Release 6.1(3x) includes the following Data Migration Assistant (DMA) enhancements. For more details, refer to the documents *Data Migration Assistant User Guide 6.1(3)* and *Upgrading to Cisco Unified Communications Manager Release 6.1(3) from Cisco Unified Communications Manager 4.x Releases*:

- The platformConfig.xml file that DMA generates supports upgrades for the first node (publisher database server) as well as for the subsequent nodes (subscribers). DMA provides a window where you can make detailed configuration specifications. Enter data at the DMA window Export > Answer File Generator.
- DMA provides a window where users can customize the behavior of DMA by specifying which types of logs to include in the output file. Enter data at the DMA window Export > Custom Options
- DMA explicitly lists the pre-DMA export tasks. DMA provides both information and the automation of pre-export tasks when possible to ensure that they know what tasks they need to complete before DMA is run. Enter data at the DMA window Export > Pre-Export Tasks.
- DMA supports the generation of a license file upon successful DMA validation. The user can upload this license file to Cisco CCO to get the actual license file ready for use. Go to the DMA window Export > Storage Location and specify a local directory destination for the license file licupgrade.lic Specify the destination in the “Path Name” text box of the window’s “Destination Option for License File” field.

For More Information

- Effects on CAR Data When You Upgrade Cisco Unified Communications Manager by Using Data Migration Assistant, page 66
- Ensure CAR Administrator Privileges Are Restored After Upgrade, page 67

Command Line Interface

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

Spaces in File Names

For Cisco Unified Communications Manager Release 6.1(3x), you can use CLI commands to directly work with file names that contain spaces. For example, you could use the **file delete** command to delete a log file with the name cisco test log in the Platform directory:

file delete activelog platform cisco test log

Relative Paths

When you download a file to your local computer with the **file get** command, the system prompts you to enter a download directory. For Cisco Unified Communications Manager Release 6.1(3x), you can specify a relative path for the download directory by using the **./** notation, as shown in the following example:

Download directory: ./RepStat

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

New Commands and Parameters

This section provides information about the following new CLI command for Cisco Unified Communications Manager Release 6.1(3x):

utils create report csa

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

For more information about command syntax and parameters, see Appendix A of the *Cisco Unified Communications Operating System Administration Guide* and the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

New and Updated Enterprise and System Parameters

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

Enterprise Parameters

No enterprise parameters updates occurred for Cisco Unified Communications Manager 6.1(3x).

Service Parameters

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

- Party Entrance Tone—This parameter supports the Cisco CallManager service for the"Viewing Held Calls on Shared Lines" feature.

- Always Use Prime Line—This parameter supports the Cisco CallManager service for the "Always Use Prime Line" feature.
- Always Use Prime Line for Voice Message—This parameter supports the Cisco CallManager service for the "Always Use Prime Line for Voice Message" feature.
- Table Out Of Sync—This parameter supports the Cisco CallManager service for the "Table Out of Sync Detection" feature.
- Enable Transit Counter Processing on QSIG Trunks—This parameter supports the Cisco CallManager service for the "Transit Counter That is Implemented in Codeset5 for QSIG PRI Trunks" feature.
- Send Multicast MOH in H.245 OLC Message—This parameter supports the Cisco CallManager service for the "Multicast Music On Hold Over H.323/SIP Trunk" feature.

Menu Changes

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

Main Window

After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For more information, see the "Licensing Enhancements" section on page 45.

System

The System menu contains the following changes:

- System > Service Parameters —For information on new or updated service parameters, see the "New and Updated Enterprise and System Parameters" section on page 29.
- System > Licensing > License File Upload—This window displays a message that uploading the license file removes the demo licenses for the feature. For more information, see the "Licensing Enhancements" section on page 45.
- System > Licensing > License File Upload—This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded. For more information, see the "Licensing Enhancements" section on page 45.

Call Routing

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

- Call Routing > Directory Number—The Log Missed Calls check box displays, as described in the "Logging Missed Calls For Shared Lines" section on page 46.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

The Device menu displays the following new and updated settings.

- Device > Phone—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.
- Device > Device Settings > Default Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.
- Device > Device Settings > Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.
- Device > Device Settings > Common Phone Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.

Application

No updates or new fields exist for this menu.

User Management

No changes exist for the User Management menu.

Bulk Administration

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

- Bulk Administration > Phones > Phone Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.
- Bulk Administration > User Device Profile > UDP Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.
- Bulk Administration > Phones > Update Phones—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 33. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 36.

- Bulk Administration > Phones > Phone Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays, as described in the "Logging Missed Calls For Shared Lines" section on page 46.
- Bulk Administration > User Device Profile > UDP Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 46.
- Bulk Administration > Phones > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 46.
- Bulk Administration > User device Profiles > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 46.
- Bulk Administration > Phones > Phone Template Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Support for Party Entrance Tone" section on page 59.
- Bulk Administration > User Device Profile > UDP Template Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Support for Party Entrance Tone" section on page 59.
- Bulk Administration > Gateways > Gateway Template. Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Support for Party Entrance Tone" section on page 59.
- Bulk Administration > Gateways > Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box, as described in the "Support for VG202 and VG204 Gateways" section on page 62.
- Bulk Administration > Gateways > Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box as described in the "Support for VG202 and VG204 Gateways" section on page 62.
- Bulk Administration > Gateways > Insert Gateways. Select Gateway type and click next. The second Insert Gateways Configuration window displays—Sample insert gateways link now displays VG202 and VG204 sample files along with other BAT supported gateways, as described in the "Support for VG202 and VG204 Gateways" section on page 62.

Cisco Unified Communications Manager Features and Applications

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

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

Always Use Prime Line

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

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

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

Cisco Unified Communications Manager Administration Configuration Tips

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

For more configuration considerations, see Table 5 on page 34.

GUI Changes

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

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

For information on how the Always Use Prime Line setting works when a phone idle or busy, see Table 5 on page 34.

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

Table 5 Always Use Prime Line for Voice Message Configuration

State of Phone	Configuration for Always Use Prime Line	How Feature Works
Idle	On	When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. If you choose On for the Always Use Prime Line for Voice Message setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received; that is, when the phone is off hook.
Idle	Default	If you choose Default for the Always Use Prime Line setting in the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when determining whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	When the phone already has a call on a line, Cisco Unified Communications Manager uses the configuration for the Maximum Number of Calls and Busy Trigger settings to determine how to route the call.
Idle	On, but you also configured Auto Answer With Headset or Auto Answer with Speakerphone	If you choose the Auto Answer with Headset option or Auto Answer with Speakerphone option from the Auto Answer drop-down list box in Cisco Unified Communications Manager Administration, the Auto Answer configuration overrides the configuration for the Always Use Prime Line setting.

Service Parameter and Enterprise Parameter Changes

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

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 6.1(3x), you can configure this feature per device or per device profile.

Serviceability Considerations

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

BAT Considerations

The Bulk Administration GUI has the following updates to support the Always Use Prime Line feature:

- Always Use Prime Line drop-down list box—choose one of the following options:
  - Off
  - On
  - Default

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 5.

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

- Insert, Export, and Validate Details support for always use prime line—the following insert, export, and validate details features have support for the always use prime line feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details

  - Insert Phones/Users
  - Validate Phones/Users
- UDP File Format—UDP File Format Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Device Fields section.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 88.

For More Information

- Always Use Prime Line for Voice Message, page 36
- Line Select, page 88

Always Use Prime Line for Voice Message

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

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

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

Cisco Unified Communications Manager Administration Configuration Tips

For configuration considerations, see Table 6 on page 37.

GUI Changes

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

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

For information on how the Always Use Prime Line for Voice Message setting works when a phone is idle or busy, see Table 6 on page 37.

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

Table 6 Always Use Prime Line for Voice Message Configuration

State of Phone	Configuration for Always Use Prime Line for Voice Message	How Feature Works
Idle	On	If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. If you choose On for the Always Use Prime Line for Voice Message setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message.Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.

Table 6 Always Use Prime Line for Voice Message Configuration

State of Phone	Configuration for Always Use Prime Line for Voice Message	How Feature Works
Idle	Default	If you choose Default for the Always Use Prime Line for Voice Message setting in the Phone Configuration, the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter when it determines whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line for Voice Message setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	If the device is busy, this feature does not work.

Service Parameter and Enterprise Parameter Changes

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

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 6.1(3x), you can configure this feature per device.

Serviceability Considerations

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

BAT Considerations

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

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

- Off
- On
- Default

Note For details of configuration options for the Always Use Prime Line for Voice Mail feature, refer to Table 6.

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

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 88.

For More Information

- Always Use Prime Line, page 33
- Line Select, page 88

Barge, cBarge, and Single Button Barge Support for PLAR

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

Barge, cBarge, or single-button barge allow a phone user to get added to a remotely active call that is on a shared line. Private Line Automatic Ringdown (PLAR) allows the phone user to dial a preconfigured number, and only this number, from the PLAR line. In Cisco Unified Communications Manager 6.1(3x), a barge, cBarge, or single-button barge initiator can barge into a call via a shared line that is configured for PLAR; that is, the initiator can barge into the call if the barge target uses the preconfigured number that is associated with the PLAR line while on the call.

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

Cisco Unified Communications Manager Administration Configuration Tips

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

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

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

Example for How to Configure PLAR

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

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

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

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

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

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

GUI Changes

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

Service Parameter and Enterprise Parameter Changes

For parameters that you configure for barge, refer to the "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide* and the "Party Entrance Tone" section on page 51.

Installation/Upgrade (Migration) Considerations

You can use this feature after you install or upgrade to Cisco Unified Communications Manager 6.1(3x).

Serviceability Considerations

No special serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

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

For a list of phones that support this feature, see the "Barge Tone Enhancements" section on page 85.

For More Information

- "Barge and Privacy," *Cisco Unified Communications Manager Administration Guide, Release 6.1(1)*
- Party Entrance Tone, page 51
- Barge Tone Enhancements, page 85

Cisco Unified Communications Manager Assistant

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Cisco Unified Communications Manager Release 6.1(3x) supports numeric user ID login for Cisco Unified Communications Manager Assistants from their Cisco Unified IP Phones.

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

Procedure

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

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

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

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

Cisco Web Dialer Configured in Application Server Window

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

In previous releases of Cisco Unified Communications Manager, the List of WebDialers field in the Service Parameter window supported a maximum of 255 characters, which limited the scalability of the Redirector. In Cisco Unified Communications Manager 6.1(3x), you configure the Web Dialer servers in the Application Server Configuration window instead of the Service Parameters Configuration window.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

It is now possible for you to add a Cisco Web Dialer application server through the Application Server Configuration window. You access the Application Server Configuration window by choosing **System > Application Server** in Cisco Unified Communications Manager Administration. Cisco Web Dialer appears as one of the options in the Application Server Type drop-down list box.

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

Service Parameter and Enterprise Parameter Changes

In Cisco Unified Communications Manager 6.1(3x), you can configure either the List of WebDialers service parameter or the Cisco Web Dialer application server through the Application Server Configuration window. If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service. You can access the Service Parameter Configuration window by choosing **System > Service Parameters** in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

If you configured the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service before the upgrade to Cisco Unified Communications Manager 6.1(3x).

If you install Cisco Unified Communications Manager 6.1(3x) and plan to use Cisco Web Dialer, configure the Cisco Web Dialer application server in the Application Server Configuration window. You do not need to configure the List of WebDialers field in the Service Parameter Configuration window if you configure the application server in the Application Server Configuration window.

Serviceability Considerations

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

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

See the "Cisco Web Dialer API" section on page 83.

User Tips

For user enhancements for Cisco Web Dialer, see the "Web Dialer Enhancements" section on page 91.

For More Information

- "Cisco Web Dialer" chapter, *Cisco Unified Communications Manager Features and Services Guide*, Release 6.1(1)
- Web Dialer Enhancements, page 91

Location-Based Call Admission Control Over Intercluster Trunk

Description

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

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

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

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

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

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

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

Cisco Unified Communications Manager Administration Configuration Tips

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

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

Caution If the ICT or H323 gateway is placed in a user defined location other than the Phantom location, this feature will not work. Also, if the ICT is connected to third-party system that does not recognize and pass the Cisco specific Location information in the SIP or H323 signals, this feature will not work

GUI Changes

This feature does not entail any new menu options or new fields in Cisco Unified Communications Manager Administration. The Phantom value is added for all entities that specify a location in the Location drop-down list box. Find the Location field on the Device Pool Configuration, Annunciator Configuration, Music On Hold (MOH) Server Configuration, Conference Bridge Configuration, Voice Mail Port Configuration, Voice Mail Port Wizard Configuration, CTI Route Point Configuration, Gateway Configuration, Phone Configuration, Trunk Configuration, and Pilot Point Configuration windows.

Service Parameter and Enterprise Parameter Changes

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

Installation/Upgrade (Migration) Considerations

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

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL nor CTI considerations exist for this feature.

User Tips

This feature does not entail user interaction.

For More Information

- Call Admission Control, *Cisco Unified Communications Manager System Guide, Release 6.1(1)*
- Resource Reservation Protocol, *Cisco Unified Communications Manager System Guide*, *Release 6.1(1)*
- Understanding Cisco Unified Communications Manager Trunk Types, *Cisco Unified Communications Manager System Guide*, *Release 6.1(1)*
- Location Configuration, *Cisco Unified Communications Manager Administration Guide*, *Release 6.1(1)*

Licensing Enhancements

Description

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

Cisco Unified Communications Manager Administration Configuration Tips

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

GUI Changes

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

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

Service Parameter and Enterprise Parameter Changes

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

Installation/Upgrade (Migration) Considerations

After you upgrade to Cisco Unified Communications Manager 6.1(3x) from a compatible Cisco Unified CM 5.x or 6.x release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated.

When you upgrade from any supported release of Cisco Unified Communications Manager to Release 6.1(3x), you must download and install a software feature license to activate the new features. The Cisco Unified Communication Administration Guide indicates that you must install a software feature license only if you are upgrading from 5.x or 6.x releases. You also need a license if you are upgrading from supported 4.x releases. For instructions about how to obtain and install a software feature license, see the "License File Upload" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Immediately after you complete the upgrade to Cisco Unified Communications Manager 6.1(3x), upload the software feature license that is required for Cisco Unified Communications Manager 6.1(3x) in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 6.1(3x).

For more information, see Data Migration Assistant (DMA) Enhancements, page 28.

Serviceability Considerations

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

BAT Considerations

No BAT considerations exist for these licensing enhancements.

CAR/CDR Considerations

No CAR or CDR considerations exist for these licensing enhancements.

Security Considerations

No security considerations exist for these licensing enhancements.

AXL and CTI Considerations

No AXL or CTI considerations exist for these licensing enhancements.

User Tips

This feature does not impact the end user.

For More Information

- "Licensing" chapter, *Cisco Unified Communications Manager System Guide*, *Release 6.1(1)*

Logging Missed Calls For Shared Lines

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

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

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

The examples in Table 7, which use the following phones, describe how the missed call logging feature works for shared lines:

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

Table 7 Example of How Logging Works for Missed Calls With Shared Lines

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

Cisco Unified Communications Manager Administration Configuration Tips

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

GUI Changes

The Directory Number Configuration window in Cisco Unified Communications Manager Administration displays the Logged Missed Calls check box, which turns on or off this feature. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the

phone. To access the check box, choose **Call Routing > Directory Number**. In the Directory Number Configuration window, highlight the associated device in the Associated Devices pane; then, click the **Edit Line Appearance** button.

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

Service Parameter and Enterprise Parameter Changes

No new or updated parameters exist for this feature.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 6.1(3x) introduces this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

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

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

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

- Insert, Export, and Validate Details support for the log missed calls feature—the following insert, export, and validate details features have support for the log missed calls feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
- File Formats—the following file formats support the Log Missed Calls feature:
  - Phone File Format—Log Missed Calls field represents a part of the Line Fields section.

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

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

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

For a list of phone models that support this feature, see the "Missed Calls" section on page 89.

For More Information

- Missed Calls, page 89

Multicast Music On Hold Over H.323/SIP Trunk

Description

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

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

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

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

Cisco Unified Communications Manager Administration Configuration Tips

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

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

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

GUI Changes

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

Service Parameter and Enterprise Parameter Changes

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

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

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

Installation/Upgrade (Migration) Considerations

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

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL considerations exist for this feature.

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

User Tips

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

For More Information

- Music on Hold, *Cisco Unified Communications Manager Features and Services Guide, Release 6.1(1)*

Party Entrance Tone

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

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

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

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

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

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

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

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

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

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

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

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

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

Service Parameter and Enterprise Parameter Changes

For this location-based parameter, configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service. To access this parameter, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration; choose the server and the **Cisco CallManager** service. When the parameters display, locate the Party Entrance Tone service parameter. For more information on this parameter, click the name of the service parameter or the question-mark button in the Service Parameter Configuration window.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 6.1(3x) introduces this feature.

Serviceability Considerations

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

BAT Considerations

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

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

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

Note The Party Entrance Tone drop-down list box exists on the Phone Line Template, UDP Line Template, UDP Update Line, RDP Line Template, Phone Update Line, and UDP Update Line window.

- For information regarding Insert, Export, and Validate Details support for party entrance tone "Support for Party Entrance Tone" section on page 59.
- For more information on BAT, refer to the Bulk Administration Tool section of this document.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For information on the phones that support this feature, see the "Barge Tone Enhancements" section on page 85.

For More Information

- Barge Tone Enhancements, page 85

Table Out of Sync Detection

Note The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration.

Description

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

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

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

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

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

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

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

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

Step 4 Set the Maintenance Time parameter value.

Step 5 Set the Maintenance Window parameter value.

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

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

Step 8 Click **Save**.

Steps to Ensure That You Are Notified of Inconsistencies

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

- Complete the steps that are described in "Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes" section on page 54.
- Enable the alert.
- Configure the Alert in RTMT.

Enable the Alert

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

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

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

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

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

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

Step 6 Click **Save**.

Configure the Alert in RTMT

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

Note You can configure RTMT to alert you via email.

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

For More Information

- *Cisco Unified Real-time Monitoring Tool Guide*

Transit Counter That is Implemented in Codeset5 for QSIG PRI Trunks

An IE that Q.931 supports, called Transit Counter, stops routing loops on PBXs.

The transit counter information element specifies a maximum length of 3 octets and may get included in the setup message. It indicates the number of private network transit exchanges that occur in a requested connection.

Cisco Unified CM parses a transit counter that is received in a setup message on a QSIG Trunk (as well as Annex M.1) when it is received in locking codeset5 and sends it to call control. If the subsequent leg of the call is QSIG , that leg increments the received transit counter and sends it outbound over QSIG (and Annex M.1) in locking codeset5.

Note Cisco Unified CM does not make route loop decisions that are based on transit counter information. It only transits and increments the counter.

A new service parameter, Enable Transit Counter Processing on QSIG Trunks, controls this implementation.

When the service parameter is set to false, the Unified CM

- Behaves as it did in previous releases.
- Does not send out the transit counter IE.

When the service parameter is set to true, the Unified CM

- Only increments it in transit situations.
- Never originates a transit counter.

Unconfigured Device Registration Attempts Restricted

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

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

Supported Devices

The following devices support this changed registration behavior:

- IP Phone 7906G

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

For more information, refer to the *Cisco Unified IP Phone Administration Guide.*

Cisco Unified Communications Manager Administration Configuration Tips

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

Before you configure a phone, consider the following information:

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

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

  For a phone that uses the dummy MAC address that is created via BAT, the Is Active check box displays as unchecked and enabled. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, check the Is Active check box, which ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone.
- Cisco Unified Communications Manager allows you to provision phones with dummy MAC addresses via BAT as long as the number of used device license units and the number of pending device license units do not exceed the total number of device license units that are available for use.

- If you use the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS) to associate an auto-registered phone with the BAT dummy settings, the Cisco Unified Communications Manager Auto-Register Phone Tool deletes the auto-registered phone from the database, and licensing gives you credits for the device license units for the deleted phone. After the Cisco Unified Communications Manager Auto-Register Phone Tool applies the device name to the phone that uses the dummy MAC address, the Cisco Unified Communications Manager Auto-Register Phone Tool updates the Is Active check box to display as checked and disabled. Licensing consumes device license units for the phone, and the phone can register with Cisco Unified Communications Manager, unless the number of used device license units exceeds the total number of device license units that are available for use.
- When a phone auto-registers for use with the Cisco Unified Communications Manager Auto-Register Phone Tool, it gets inserted into the database as long as the number of used device license units is less than the number of device license units that are available for use.
- You can view the number of pending, used, and available device license units in the License Unit Report and the License Unit Calculator in Cisco Unified Communications Manager Administration.

GUI Changes

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

Service Parameter and Enterprise Parameter Changes

No parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 6.1(3x), if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager.

Serviceability Considerations

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

BAT Considerations

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

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

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

Viewing Held Calls on Shared Lines

Tip The information in this section does not exist in the online help for Cisco Unified Communications Manager Administration or in any other Cisco Unified Communications Manager 6.1(x) document besides the release notes.

Description

With the held calls on shared lines feature, a phone user can determine whether the call was put on hold by the phone user locally at the primary device or by another party remotely on a shared device. How the held call displays on the devices depends on whether the primary device or shared device puts the call on hold. For information on how the held call displays on the devices, see the "Hold Status" section on page 87.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

This feature requires no configuration to work.

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 6.1(3x) introduces this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Hold Status" section on page 87.

For More Information

- Hold Status, page 87

Bulk Administration Tool

This section contains information on the following topics:

Support for Party Entrance Tone

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

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

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

- Insert, Export, and Validate Details support for party entrance tone—The following insert, export, and validate details features have support for the party entrance tone:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Insert Gateways

  - Insert Remote Destination Profiles
  - Export Remote Destination Profiles
  - Phone Add lines
  - Phone Update Lines
  - UDP Update Lines
  - UDP Add Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—The following file formats support the party entrance tone feature:
  - Phone File Format—Party Entrance Tone field represents a part of the Line Fields section.
  - UDP File Format—Party Entrance Tone field represents a part of the Line Fields section.
  - Remote Destination Profile File Format—Party Entrance Tone field represents a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Party Entrance Tone field in the Line Fields section.
- Generate Phone Report—The Generate Phone Report Configuration page lists the Party Entrance Tone field in the Line Fields section.

Support for Log Missed Calls

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

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

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

- Insert, Export, and Validate Details support for the log missed calls feature—The following insert, export, and validate details features have support for the log missed calls feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details

  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Phone Add lines
  - Phone Update Lines
  - UDP Update Lines
  - UDP Add Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—The following file formats support the log missed calls feature:
  - Phone File Format—Log Missed Calls field represents a part of the Line Fields section.
  - UDP File Format—Log Missed Calls field represents a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Log Missed Calls field in the Line Fields section.
- Generate Phone Report—The Generate Phone Report Configuration window lists the Log Missed Calls field in the Line Fields section.

Support for Always Use Prime Line

The Bulk Administration GUI has the following updates to support the Always Use Prime Line feature:

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

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 5 and Table 6.

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

- Insert, Export, and Validate Details support for always use prime line—The following insert, export, and validate details features have support for the always use prime line feature:
  - Insert Phones Specific Details

  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Generate Phone Report
  - Generate UDP Report
- Phone File Format—Phone File Format Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- UDP File Format—UDP File Format Configuration window lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Device Fields section.
- Generate Phone Report—The Generate Phone Report Configuration window lists the Always Use Prime Line and Always Use Prime Line for Voice Message fields in the Device Fields section.

Support for VG202 and VG204 Gateways

BAT now supports VG202 and VG204 gateways. The Bulk Administration Tool has the following updates to support VG202 and VG204 gateways:

- Bulk Administration > Gateways > Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration > Gateways > Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration > Gateways > Insert Gateways. Select Gateway type as VG202 or VG204 and click next. The second Insert Gateways Configuration page displays—The View Sample File link displays VG202 and VG204 sample files.
- File Formats—the Create File Format and Add File Format gateway windows now support VG202 and VG204 gateways.
- Generate Gateway Report—The Generate Gateway Report Configuration windows now lists all BAT supported gateways including VG202 and VG204.
- Delete Gateway—The Delete Gateways Configuration window now lists all BAT supported gateways including VG202 and VG204.

- BAT.XLT Support—BAT.XLT supports VG202 and VG204 gateways.

Cisco Unified Serviceability

The following sections comprise new and changed features in serviceability for Unified CM 6.1(3x).

DBReplicationTableOutOfSync Alarm

In Cisco Unified Serviceability, you can configure the DBReplicationTableOutOfSync alarm, as described in the "New Preconfigured Alert - DBReplicationTableOutOfSync" section on page 64.

Cisco UXL Web Service Added to Service Activation Window

In most Cisco Unified Communications Manager releases, the TabSync client in Cisco IP Phone Address Book Synchronizer uses AXL for end-user queries to the Cisco Unified Communications Manager database. In Cisco Unified Communications Manager 6.1(3x), the TabSync client uses the Cisco UXL Web Service for queries to the Cisco Unified Communications Manager database, which ensures that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them.

In the Service Activation window in Cisco Unified Serviceability (Tools > Service Activation), you can activate the Cisco UXL Web Service, which performs the following functions:

- Conducts authentication checks by verifying the end user name and password when an end user logs in to Cisco IP Phone Address Book Synchronizer.
- Conducts a user authorization check by only allowing the user that is currently logged in to Cisco IP Phone Address Book Synchronizer to perform functions such as listing, retrieving, updating, removing, and adding contacts.

Cisco Unified Real-Time Monitoring Tool

This section contains information on the following topics:

Quality Report Tool Reports

A change occurred in the Call State information that is collected from Cisco Unified Communications Manager/CTIManager and displayed in the Quality Report Tool (QRT) reports. Previously, the information included Connected, Connected Conference, Connected Transfer, and On Hook call state information. Now, the report only includes Connected and On Hook call state information.

New Preconfigured Alert - DBReplicationTableOutOfSync

For information on the DBReplicationTableOutofSync alert, see the "Table Out of Sync Detection" section on page 53.

System History Log Displays in RTMT

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

RTMT > Trace Log Collection

For more information on the system history log, see the "System History Log for Cisco Unified Communications Manager" section on page 25.

Cisco Unified Communications Manager CDR Analysis and Reporting

This section contains these subsections:

Configuring Department Bills Reports

The following additional note applies to Step 6 of the Configuring Department Bills Reports procedure:

Click the **Down** radio button to view your direct reports. Use the **Up** and **Down** radio buttons to move up and down the report chain.

Reports That Are Unavailable to Administrator While CAR Database Gets Manually Purged or CDR Records Get Reloaded

A CAR administrator can no longer generate CAR reports when a manual purge of the CAR database is in process or CDR records are reloading. The following message displays when you try to run reports during these processes:

```
10023: Manual Purge/Reload is in process. Please run the reports once the Manual
Purge/Reload is over.
```

Both the Purge button and the Reload All Call Detail Records button get disabled, and the following message displays on the Manual Purge window, when either a manual purge or CDR reload occurs:

```
Manual Purge/Reload is still running. User will not be allowed to run another instance of
Manual Purge/Reload. So, both Purge and Reload All Call Detail Records buttons are
disabled.
```

Before this enhancement, a CAR administrator could request CAR reports during the purge, but message 10012 displayed.

SIP Call with URL as Extension Number Now Supported

Because calling and called parties can have SIP calls where the extension number is a URL, you can use all printable ASCII characters in the extension number. No space gets allowed in the URL. For example, extension "1000 1001" does not get accepted as a valid URL. The following message displays:

```
30035 Invalid extension number.
```

Note Printable ASCII characters comprise characters with ASCII code (in decimal) 33 through 126.

CDR Search by User Extension Supports "+" and URLs for SIP Calls

When you use the CDR Search by User Extension feature, you may use the "+" in any position of the user extension number; however, in the current release of Cisco Unified Communications Manager and previous releases, the "+" cannot be used in any dial plan configurations.

When the user extension number is a SIP call with a URL, the system allows no space in the URL.

Changes to Mail Server Configuration GUI

You must now configure the mail ID, mail domain, and mail server name when you configure the mail server. Previously, you only had to configure the mail ID.

Procedure

Step 1 Choose **System > System Parameters > Mail Parameters**.

The Mail Parameters window displays.

Step 2 In the Mail ID field, enter the e-mail identifier that will be used in the From field when e-mails are sent (for example, smith1@abc.com, enter **smith1** in the Mail ID field).

Note CAR does not support SMTP authentication. You must disable authentication on the SMTP mail server.

Step 3 The Password field and the Confirm Password field automatically get populated with the user password information.

Step 4 In the Mail Domain field, enter the domain name for the server that runs the e-mail system (that is, **abc.com** from the example in Step 2).

Step 5 In the Mail Server Name field, enter the mail server name or the IP address where the mail server runs (for example, 192.168.10.0)

Note You must provide entries in the Mail ID, Mail Domain, and Mail Server Name fields.

Step 6 To make the changes, click the **Update** button.

Change in Supported FTP/SFTP Versions for CAR Billing Servers

Cisco allows you to use any SFTP server product but Cisco recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner (CTDP) program.

CTDP partners, such as GlobalSCAPE, certify their products with a specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://www.cisco.com/pcgi-bin/ctdp/search.pl. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx. Cisco uses the following servers for internal testing. You may use one of these servers, but you must contact the vendor for support:

- Open SSH (for Unix systems)
- Cygwin (Refer to http://sshwindows.sourceforge.net/.)
- Titan (Refer to http://www.titanftp.com/.)

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

Cisco has tested and will support the following versions of FTP or SFTP for CAR billing servers:

Linux/Unix

FTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)

SFTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)

Windows

FTP: Microsoft FTP service (Windows 2000 5.00.2195 sp4, IIS 5.0) and WAR FTP Daemon (1.82.0.10)

Effects on CAR Data When You Upgrade Cisco Unified Communications Manager by Using Data Migration Assistant

If you do not need to carry over your CAR data to Cisco Unified Communications Manager 6.1(3x), Cisco recommends that you purge the CAR data before you run the Data Migration Assistant (DMA). Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.

Note Make sure that you purge any CAR records that are older than 180 days.

The Cisco Unified Communications Manager installation program limits the time in which CAR records migrate from the DMA TAR file to the CAR database on the upgraded system. The time limit that is allotted for the CAR component specifies 60 minutes. So, to facilitate migration of more data within the stipulated time, CAR uses the following logic:

- Data migration starts with the migration of billing records from the tbl_billing_data CSV file into the tbl_billing_data table of the CAR database. Data migration starts from the latest record and proceeds toward the oldest record in the CSV file. The billing data migration stops when no more billing records remain to be migrated or the 60-minute time limit is reached, whichever occurs first.
- After the billing data migration, if time remains in the preallotted 60-minutes, CAR proceeds with migration of error records from the tbl_billing_error CSV file into the tbl_billing_error table of the CAR database. Data migration starts from the latest record and proceeds toward the oldest record in the CSV file. For each error record that is migrated, CAR migrates the data that corresponds to the error_record_id that is present in the tbl_error_id_map CSV file into the tbl_error_id_map table of the CAR database. This action ensures that error record migration stays consistent with data in the tbl_error_id_map. The migration process continues until no more data remains to migrate or the 60-minute time limit gets reached, whichever occurs first.
- Whenever the time limit gets reached, CAR data migration stops, and the tbl_system_preferences of the CAR database gets updated to reflect the data present in the upgraded system database.

Note If you upgrade from Cisco Unified Communications Manager 4.x, Cisco Unified Communications Manager saves the content of the Cisco Unified Communications Manager 4.x CAR database to CSV files. The Cisco Unified Communications Manager 4.x CAR database has part of the CDR information. The Cisco Unified Communications Manager 4.x CDR database stores the complete information about CDRs. This database does not migrate. The Data Migration Tool uses the CAR database CSV files to migrate the CAR database. The system stores the CSV files in the /common/download/windows/car directory. The system stores the pregenerated reports in the /common/download/windows/pregenerated database. Because no corresponding CDR database exists in Cisco Unified Communications Manager 5.x and later releases, the complete CDR data does not migrate to the Cisco Unified Communications Manager 5.x or 6.x system. The Cisco Unified Communications Manager 5.x and 6.x CAR database schema gets extended to contain complete CDR information, but only for the new CDRs that the Cisco Unified Communications Manager 5.x and 6.x system generates.

Ensure CAR Administrator Privileges Are Restored After Upgrade

When you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. You must reset the CAR administrator privileges after the upgrade. Refer to the “Configuring CAR Administrators, Managers, and Users” section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.

Configuring CDR Error Reports

To determine why the error records fail the CDR load, you must review the information in the tbl_error_id_map table.

Table 8 lists the CDR error codes and the definition of the error.

Table 8 CDR Error Codes

Error Code	Definition
CDRs	
31101	CDR globalCallID_callManagerId <= 0
31102	CDR globalCallID_callId <= 0
31103	CDR origLegCallIdentifier <= 0
31105	CDR dateTimeOrigination <= 0
31108	CDR destLegIdentifier <= 0
31110	CDR dateTimeConnect <= 0
31111	CDR dateTimeDisconnect <= 0
31119	CDR originalCalledPartyNumber is empty
31120	CDR finalCalledPartyNumber is empty
31122	CDR duration < 0
31137	CDR LDAP error while retrieving UserID or ManagerID
31139	CDR callingPartyNumber is empty
31147	CDR origDeviceName is empty
31148	CDR destDeviceName is empty
31151	CDR origCallTerminationOnBehalfOf < 0
31152	CDR destCallTerminationOnBehalfOf < 0
31153	CDR lastRedirectRedirectOnBehalfOf < 0
31155	CDR destConversationId < 0
31156	CDR globalCallId_ClusterID is empty
Orig CMR	
31123	Orig CMR globalCallID_callManagerId <= 0
31124	Orig CMR globalCallID_callId <= 0
31125	Orig CMR numberPacketsSent < 0
31126	Orig CMR numberPacketsReceived < 0
31127	Orig CMR jitter < 0
31129	Orig CMR callIdentifier <= 0
31149	Orig CMR deviceName is empty
31157	Orig CMR globalCallId_ClusterID is empty
Dest CMR	
31140	Dest CMR globalCallID_callManagerId <= 0
31141	Dest CMR globalCallID_callId <= 0
31142	Dest CMR numberPacketsSent < 0
31143	Dest CMR numberPacketsReceived < 0
31144	Dest CMR jitter < 0

Table 8 CDR Error Codes (continued)

Error Code	Definition
31145	Dest CMR callIdentifier <= 0
31150	Dest CMR deviceName is empty
31158	Dest CMR globalCallId_ClusterID is empty

Event Log Report Status

A new field has been added to the Event Log report status: Scheduled—If this check box is checked, the event log report includes tasks that have been scheduled but have not yet started.

When the Scheduler restarts, all unfinished jobs with a status of Scheduled get deleted. Current jobs with the status of In Progress or Scheduled get changed to Unsuccessful.

New Error Message That Is Introduced If Data Present in Invalid or Remainder Partitions

A message gets logged in the CAR Scheduler traces if data is present in invalid and remainder partitions of the tbl_billing_data and tbl_billing_error files.

The LWM/HWM/2M e-mail alerts that get sent to the CAR administrator when CAR detects records in either the part_invalid or part_remainder partitions will contain the following information:

```
Data is present in invalid/remainder partition also, which cannot be removed by
Automatic-Purge. Please delete these record(s) manually from Manual-Purge.
```

Configuring Individual and Department Bills Reports

Before you can configure the Individual Bills report, you must ensure that a device with an assigned Owner User ID exists in Cisco Unified Communications Manager Administration for each user that is included in the report. Use the following procedure to create the Owner User IDs:

Procedure for Adding Owner User ID to Individual Bills

In Cisco Unified Communications Manager Administration, choose **Device > Phone > Add a New Phone > Phone Configuration**.

Add the information for the device and the user.

Before you can configure the Department Bills report, you must ensure that a device with an assigned Owner User ID and Manager User ID exists in Cisco Unified Communications Manager Administration for each user that is included in the report. Use the following procedure to add the device, Owner User ID, and the associated Manager UserID for each user:

Procedure for Adding Owner User ID and Manager ID to Department Bills

In Cisco Unified Communications Manager Administration, choose **Device > Phone > Add a New Phone > Phone Configuration**.

Add the information for the device and the user.

In Cisco Unified Communications Manager Administration, choose **User Management > End User > Add**.

Add the Manager User ID information to the end user information.

For both individual bills and department bills, if the Extension Mobility feature is enabled on the device and the user logs in to the phone and places a call, the User ID that gets recorded in the CDRs represents the logged in User ID. If Cisco Extension Mobility is not enabled on the device, the User ID that gets recorded in the CDRs specifies the Owner User ID that is configured for the device. In the situation where neither the User ID or the Owner User ID is configured (that is, Cisco Extension Mobility is not enabled, and the Owner User ID is not configured), the User ID field in the CDRs gets recorded as blank. In this situation, CAR uses the default User ID of "_unspecified user" when it loads the CDRs, and the CDRs do not display in the Individual Bills User reports because no user by the name of "_unspecifieduser" exists in the Cisco Unified Communications Manager database. If you look for the reports for a particular end user in the directory, either the User ID for the particular end user must be configured as the Owner User ID for the device or the particular end user must have logged in to the device with the Cisco Extension Mobility feature enabled.

Cisco Unified Communications Manager Call Detail Records

This section contains these subsections:

Updated Information on Global Call ID CDR Field

For Cisco Unified Communications Manager Release 5.x and later releases, the value in the GlobalCallId CDR field survives over Cisco Unified Communications Manager restarts. In Release 4.x and earlier releases, even though the GlobalCallId field is time-based, the field gets reused under conditions of heavy traffic. Because of this behavior, problems can occur with customer billing applications and the ability of CAR to correlate CMRs with CDRs and to correlate conference call CDRs. For Release 5.x and later releases, GlobalCallId redesign ensures the field retains a unique value, at least for a certain number of days. Now, the last used globalCallId_callId value gets written to disk periodically (for every x number of calls). The value gets retrieved after a Cisco Unified Communications Manager restart, and the new globalCallId_callId value begins with this number plus x.

CallingPartyNumber CDR Field Not Affected by Direct Calls

When the **Add Incoming Number Prefix to CDR** service parameter gets set to True, type of number provides the basis for the prefixing digits that get configured. Setting this service parameter to True prefixes only the following prefixing (advanced) service parameters, based on the type of number for the incoming call:

- Incoming calling party national number prefix.
- Incoming calling party international number prefix.
- Incoming calling party subscriber number prefix.
- Incoming calling party unknown number prefix.

Note Setting the **Add Incoming Number Prefix to CDR** service parameter to True has no effect if translation occurs at the translation pattern level.

For normal calls, without any redirection or split/join in case of feature interaction, the CDR entry for the CallingPartyNumber field remains the same as the incoming number. But for pickup calls (one-touch), the CallingPartyNumber field in the CDR gets changed to the number after transformation at translation pattern level because the CallingPartyNumber field in the CDR gets updated every time a new call request or a split/join or redirection occurs. When an incoming call from a gateway occurs, the nontranslated number gets received for the CallingPartyNumber field in the CDR.

For a direct call, no split/join requests exist; therefore, the CallingPartyNumber field remains the nontranslated number. However, for a one-touch pickup call, upon pickup, the Cisco Unified Communications Manager splits the original call and the pickup call and then joins them together upon pickup. At this point, the translation pattern gets applied to the calling party, and the CDR uses the translated number for the calling party.

In the following examples, the number 89999999 has a calling party transform mask that gets entered as 0351441132. A call comes in from a PSTN from calling party 89999999 to an IP phone on the Cisco Unified Communications Manager.

CDR Example 1

The IP phone answers the call. The calling party transform mask does not get applied to the calling party number.

Field Names	CDR
globalCallID_callId	1
origLegCallIdentifier	100
destLegCallIdentifier	101
callingPartyNumber	89999999
originalCalledPartyNumber	2001
finalCalledPartyNumber	2001
origCause_Value	16
dest_CauseValue	0
duration	60

CDR Example 2

The call gets picked up by another IP phone that is using the one-touch pickup feature. The calling party transform mask gets applied to the calling party number.

Field Names	CDR
globalCallID_callId	22
origLegCallIdentifier	1
destLegCallIdentifier	2
callingPartyNumber	0351441132
originalCalledPartyNumber	2001
finalCalledPartyNumber	2002

lastRedirectDn	2001
origCause_Value	0
dest_CauseValue	16
origCalledPartyRedirectReason	0
lastRedirectRedirectReason	5
origCalledPartyRedirectOnBehalfOf	16
lastRedirectRedirectOnBehalfOf	16
duration	120

CMR Examples Provided

The following examples of CMRs get generated during a normal call (IP phone to IP phone). Normal calls log three records per call: one CDR and two CMRs (one for each endpoint).

These examples represent a call between directory number 1010 and 1014. To see a sample of the CDR that gets generated during a normal call, see the "Normal Calls" section of the latest release of the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

CMR Example

Field Names	AAC CDR
cdrRecordType	2
globalCallID_callManagerid	1
globalCallID_callId	96004
nodeId	1
callIdentifier	28141535
directoryNumber	1010
dateTimeStamp	1202412060
numberPacketsSent	358
numberOctetsSent	61576
numberPacketsReceived	351
numberOctetsReceived	60372
numberPacketsLost	1
jitter	0
latency	0
pkid	e95df5b1-2914-4a03-befb-0f58bf16392d
directoryNumberPartition	
deviceName	SEP003094C39BE7

globalCallId_ClusterId	StandAloneCluster
varVQMetrics	MLQK=0.0000;MLQKav=0.0000;MLQKmn=0.0000;MLQKmx=0.0000;MLQKvr=0.95;CCR=0.0000;ICR=0.0000;ICRmx=0.0000;CS=0;SCS=0

Video Conference Call CDR Example

Calls that are part of a video conference have multiple records logged. The number of CDR records that get generated depends on the number of parties in the video conference. One CDR record exists for each party in the video conference: one for the original placed call, one for each setup call that was used to join other parties to the video conference, and one for the last two parties that are connected in the video conference.

Therefore, for a three-party ad hoc video conference, six CDR records exist:

- 1 record for the original call
- 3 records for the parties that connected to the conference
- 1 record for each setup call
- 1 record for the final two parties in the conference

Video Conference Call CDR Example

1. Call from 2001 to 2309; 2309 answers, and they talk for 60 seconds.
2. 2001 presses the conference softkey and dials 3071111.
3. 307111 answers and talks for 20 seconds; 2001 presses the conference softkey to complete the conference.
4. The three members of the conference talk for 360 seconds.
5. 3071111 hangs up; 2001 and 2309 stay in the conference. Because only two participants remain in the conference, the conference feature joins the two directly together, and they talk for another 55 seconds.

Note Each video conference call leg gets shown placing a call into the conference bridge. The call gets shown as a call into the bridge, regardless of the actual direction of the call.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	1	2	1	1		1
origLegCallIdentifier	101	105	101	102	106	101
destLegCallIdentifier	102	106	115	116	117	102
callingPartyNumber	2001	2001	2001	2309	3071111	2001
originalCalledPartyNumber	2309	3071111	b0029901001	b0029901001	b0029901001	2309
finalCalledPartyNumber	2309	3071111	b0029901001	b0029901001	b0029901001	2309

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
lastRedirectDn	2001	3071111	b0029901001	b0029901001	b0029901001	b0029901001
origCause_Value	393216	0	16	393216	393216	16
dest_CauseValue	393216	0	393216	393216	393216	0
origVideoCap_Codec	103	103	103	103	103	103
origVideoCap_Bandwidth	320	320	320	320	320	320
origVideoCap_Resolution	0	0	0	0	0	0
origVideoTransportAddress_IP	552953152	552953152	552953152	-822647488	-945658560	552953152
origVideoTransportAddress_Port	5445	5445	5445	5445	5445	5445
destVideoCap_Codec	103	103	103	103	103	103
destVideoCap_Bandwidth	320	320	320	320	320	320
destVideoCap_Resolution	0	0	0	0	0	0
destVideoTransportAddress_IP	-822647488	-945658560	-666216182	-666216182	-666216182	-822647488
destVideoTransportAddress_Port	5445	10002	10000	10004	10001	5445
origCalledPartyRedirectReason	0	0	0	0	0	0
lastRedirectRedirectReason	0	0	0	0	0	98
origTerminationOnBehalfOf	4	4	12	12	4	12
destTerminationOnBehalfOf	4	4	0	0	4	4
origCalledRedirectOnBehalfOf	0	0	4	4	4	0
lastRedirectRedirectOnBehalfOf	0	0	4	4	4	4
joinOnBehalfOf	0	0	4	4	4	4
Conversation ID	0	1		1	1	0
duration	60	360		360	360	55

Comment	
Orig Call CDR	
Setup Call CDR	**ConfControllerDn=2001;ConfControlerDeviceName=SEP0003E333FEBD**
Conference CDR 1	ConfControllerDn=2001;ConfControlerDeviceName=SEP0003E333FEBD
Conference CDR 2	ConfControllerDn=2001;ConfControlerDeviceName=SEP0003E333FEBD

Comment	
Orig Call CDR	
Setup Call CDR	**ConfControllerDn=2001;ConfControlerDeviceName=SEP0003E333FEBD**
Conference CDR 3	ConfControllerDn=2001;ConfControlerDeviceName=SEP0003E333FEBD
Final CDR	

Cisco Unified Reporting

Cisco Unified Reporting includes a new report that indicates the number of phones with no associated users, the number of users that are associated with only one phone, and the number of users that are associated with more than one phone.

For a complete description of reports that are available on your system and the data that gets captured in a report, access the Report Descriptions report, as described in the *Cisco Unified Reporting Administration Guide*.

Cisco and Third-Party APIs

The 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.:

- Skinny Client Control Protocol (SCCP), page 75
- Administrative XML Interface, page 76
- Cisco Web Dialer API, page 83

Skinny Client Control Protocol (SCCP)

The following sections describe updates to the SCCP interface:

- BLF Enhancements, page 75
- I-Hold, page 76
- Updated SCCP Messages, page 76

BLF Enhancements

This release supports the following variations of Busy Lamp Field (BLF):

- Notification BLF Alerting—When a call arrives on a monitored line, an alerting indication notifies the monitoring stations. The alerting indication comprises a BLF icon, a flashing LED, an alerting icon, and an audible alert.
- BLF Pickup—This enhancement allows a user to pick up a call from the monitoring station during the BLF Alerting state by pressing the corresponding BLF line button.

I-Hold

This feature provides visual distinction that shows which line placed a call on hold in a shared line configuration. With this enhancement, when a call is put on hold by the local line, the current LED behavior (flashing green) continues, and the remote line changes to a flashing red LED status.

Updated SCCP Messages

This release adds, modifies, or deletes the following SCCP messages:

New messages

- StationFeatureStatV2Message—Sent from Cisco Unified Communications Manager
- StationFeatureStatReqMessage—Sent from Cisco Unified Communications Manager
- StationSetLampMessage—Sent from Cisco Unified Communications Manager
- StationStimulusMessage—Sent to Cisco Unified Communications Manager
- StationStartToneMessage—Sent from Cisco Unified Communications Manager

Modified message

- StationCallStateMessage—Modified StationDCallState ENUM

Deleted messages

- StationStartSessionTransmissionMessage
- StationStopSessionTransmissionMessage

Administrative XML Interface

The Administrative XML (AXL) interface uses the Tomcat web service that is running on the Cisco Unified Communication Manager publisher server to return client data. Several other publisher server features share this service, including Cisco Unified Communication Administration, Cisco IP Manager Assistant, Cisco Web Dialer, Cisco Extension Mobility, and the Bulk Administration Tool. The Cisco Unified Communications Manager publisher server includes enhancements that ensure that no single application can consume all available Tomcat resources.

The AXL interface now includes a throttling mechanism that limits the amount of data that client can return. The limit for data that gets returned in any single request specifies 8 MB. The limit for concurrent data requests specifies 16 MB, which can be split over any number of concurrent requests (for example, 8 concurrent requests with each requiring 2 MB of data to be returned; 4 concurrent requests with each requiring 4 MB of data to be returned; or any other combination not exceeding 8 MB per request or 16 MB concurrently).

This feature

- Prevents AXL request processing from making the Tomcat service unresponsive.
- Allows critical applications such as the Cisco Unified Communications Manager Administration interface and logging in to and out of Cisco Extension Mobility to function even when heavy AXL queries are processed.
- Allows client applications to obtain the information that is requested.
- Maximizes interface throughput.
- Minimizes required changes to existing applications.

AXL Data Throttling

The following AXL methods now include data throttling:

- executeSQLQuery
- listDeviceByNameAndClass
- listDeviceByServiceName
- listPhoneByDescription
- listPhoneByName
- listUserByName

With data throttling, the AXL interface now returns the following message when the 8-MB limit is reached: “Query request too large. Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>.”

In addition, new <skip> and <first> tags for the List X methods allow developers to fetch the data requested.

Developers who use ExecuteSQLQuery should use standard SQL Skip and First tags in the request to retrieve the desired data set.

Interaction

This section describes how the interface responds in a variety of situations.

Example 1, Option 1: Client requests data that exceeds 8 MB

Server response: ProcessingConstraintException AXL error code 5011“Query request too large. Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>”

<Number of Rows> specifies the suggested number of rows that a single request can return to keep the data exchange under the 8-MB limit. Clients should use <Matched Rows> to determine the number of iterations that are required to retrieve the complete data set that a query tries to fetch.

Client response, Option 1:

1. Client logic analyzes the server response and obtains the value of <Row Fetch>.
2. Client stores the <Row Fetch> value in a constant that depicts Row Fetch Step Size. For this example, rowFetchStepSize represents the constant name.
3. Client logic generates the request in parts based on the <Row Fetch> value.
4. Client keeps track of the number of rows that were received in the previous request. For this example, this information exists in a variable that is named prevRows.
5. Client keeps track of the total number of rows that are fetched. For this example, this information exists in a variable that is named totalRowFetch.
6. Before sending the next request, client checks whether prevRows == <Row Fetch>.
7. If the check returns true, continue the request generation loop; otherwise, break from the loop.

Example 1, Option 2: Client requests data that exceeds 8 MB

Server response: ProcessingConstraintException AXL error code 5011 “Query request too large. Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>”

<Number of Rows> specifies the suggested number of rows that a single request can return to keep the data exchange under the 8-MB limit. Clients should use <Matched Rows> to determine the number of iterations that are required to retrieve the complete data set that a query tries to fetch.

Client response, Option 2:

1. Client logic analyzes the server response and obtains the value of <Row Fetch> and <totalRows>.
2. Client stores the <Row Fetch> and <totalRows> values in variables. For this example, the variable names comprise rowFetchStepSize and countOfRows.

Note Alternatively, the client can execute a query for count(*) to obtain the number of rows that can be fetched from the database.

3. Client logic calculates the number of iterations based on the values that are stored in rowFetchStepSize and countOfRows.
4. Client logic declares two variables: “skip” (with the initial value of 0) and “first” (with initial value set to rowFetchStepSize).
5. Client starts the iteration.
6. Client logic generates the request based on “skip” and “first” at every iteration.
7. Client modifies the value of “skip” and “first” at every iteration.
8. Client checks the response at every iteration.
9. If the response is a MemoryConstraintException, the client waits until the requests in progress completes, then continues the iteration.

   If the response is not a MemoryConstraintException, the client continues the iteration.
10. Iterations continue until the <number Of Iterations> value is reached.

Example 2: Client sends single 8-MB request

Server responds with requested data.

Example 3: Client sends two 8-MB requests simultaneously

Server responds with requested data.

Example 4: Client sends more than two 8-MB requests simultaneously

The server processes the first two requests. Other concurrent requests that may be received generate this exception: MemoryConstraintException AXL error code 5009: "Maximum AXL Memory Allocation Consumed. Please retry once requests in progress have completed."

Client response:

1. Client waits for the requests that are being processed to complete and then sends the request again.

   Cisco recommends that applications wait 2 to 3 minutes before resubmitting the request.
2. Client logic must track the requests that fail and send them again.

Example 5: Concurrent data requests reach 16-MB limit

This example applies to all AXL methods.

This situation returns MemoryConstraintException AXL error code 5009: “Maximum AXL Memory Allocation Consumed. Please retry once requests in progress have completed.”

Cisco recommends that applications wait 2 to 3 minutes after receiving this message before resubmitting the request.

Using <skip> and <first> Tags in List APIs

The new <skip> and <first> tags provide additional functionality when data is retrieved by using the List methods. If a List Response exceeds 8 MB, the client can fetch data in sets of rows by using a combination of these tags. These tags provide navigation functionality. Be aware that they are not mandatory and have no default values.

In addition,

- Negative values for the <skip> or <first> tags cause a SQL syntax error.
- If the <skip> tag is not mentioned or is empty and the <first> tag is not mentioned or is empty, the default query or full query that pertains to the List API executes.
- If the <skip> tag is not mentioned or is empty and the <first> tag has some positive value (for example, “m”), a query that skips the “zero” row and fetches the first “m” rows executes.
- If the <skip> tag and <first> tag value are both positive (for example, “n” and “m,” respectively), a query that skips “n” rows and fetches “m” rows executes.

Suggested Use of <skip> and <first> Tags in List APIs

If a client request exceeds 8 MB of data, the server responds: “Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>.”

<Number of Rows> specifies the suggested number of rows that a single request can return to keep the data exchange under the 8-MB limit. Clients should use <Matched Rows> to determine the number of iterations that are required to retrieve the complete data set that a query tries to fetch.

Client response:

1. Client logic analyzes the server response and obtains the value of <Row Fetch>.
2. Client stores the <Row Fetch> value in a constant that depicts Row Fetch Step Size. For this example, the constant name specifies rowFetchStepSize.
3. Client executes a query for count(*) to obtain the number of rows that can be fetched from database. (Consider this step as required only if you are not using the exception to exit the loop.)
   a. Client modifies the tags <first> and <skip> in every iteration of the row fetch.
   b. The first iteration starts with <skip>0<skip> and <first> rowFetchStepSize</first>.
   c. Subsequent row fetch iteration have <skip>”first” tag value from previous iteration</skip> and <first>previous iteration “first” tag value + rowFetchStepSize</first>.
4. Before each iteration, client checks for the condition <skip> tag value < count(*) value. If <skip> tag value >= count(*) value, this indicates that the iteration is trying to fetch more rows than the existing number of rows in the database. In this case, break from the loop. Otherwise, the SQL Error (No Current Row) occurs, which you can use to break from loop.

Sample Code for Use of <skip> and <first> Tags in List APIs

Example 1

If the recommended RowFetch is X = 100 for ListPhoneByName, the client should use this logic:

```
StepSize = RowFetch (X = 9999)
//Two variables to store the skip and first values.
Int skip = 0;
Int first = StepSize;
//start the iteration
While (1)
{
```

```
 Try {
//A function to Modify the values of <first> and <skip> in the request with variables
values defined above
modifyRequest(FilePath);
//Sending the modified request
Response = SendExecuteSQLQuery (select SKIP <SkipCount> First <StepSize> * from endusers;)
//Modify the variables
Skip+ = StepSize;
First+= StepSize;
Check for fault_message from reply
//An SQL Exception from server while trying to fetch rows greater than that present in
database
If(fault_message .contains("No Current Row Found")){
Break;
}
Else{
Continue the loop;
}
} /* end of while*/
```

Example 2

```
#Declare variable for first and skip
long skip = 0;
long first = suggestiveRowFetch;
#Calculate number of iterations required
float precision = totalRowFetch/suggestiveRowFetch;
calculate the decimal point of variable precision
if decimal point == 0;
no. Of Iterations = totalRowFetch/suggestiveRowFetch;
if decimal point <5
no. Of Iterations = Math.round(totalRowFetch/suggestiveRowFetch)+1;
if decimal point >5
no. Of Iterations = Math.round(totalRowFetch/suggestiveRowFetch);
****Here (no. Of Iterations = 15)********
#iterator
int iLoop = 1;

while( iLoop <=no. Of Iterations){

#modify the values of first and skip in the query
String mdSQLQuery = modifySQLQuery(skip,first); /* Its like select skip 0 first 2000 *
from device for first loop*/
#send the request and get response
response = sendRequest(mdSQLQuery);
#update the skip and first variables
skip+=suggestiveRowFetch;
first+=suggestiveRowFetch;
#check for response
if(response contains MemoryConstraintException){
#undo the variable modification to get  attributes (i.e skip and first) of the query ,
that failed with an exception.
skip - =suggestiveRowFetch;
first - =suggestiveRowFetch;
wait till the requests in Progress Gets Processed;
continue the loop;

}
else{
iLoop++;
}
}
```

Sample Code for ExecuteSQLQuery

Example 1

To obtain the first X rows and then next X rows, a client should send queries as described in this section. For example, the client should use the following logic if the recommended RowFetch is X = 9999 for the query “select * from endusers;”:

```
StepSize = RowFetch (X = 9999)
SkipCount = 0
 While (1)
{
 Try {
Response = SendExecuteSQLQuery (select SKIP <SkipCount> First <StepSize> * from endusers;)
RowsReturned = Rowcount (Response);
If RowsReturned < StepSize
    Break;  /* All the rows have been fetched*/
Else
    SkipCount = SkipCount + StepSize /*Increase the SkipCount to get the next set of
rows*/
}
Catch for any exception
{
    Take appropriate action based on Exception
    Break;
}
} /* end of while*/
```

Example 2

```
#sql query to be executed
sqlQuery = "select * from device";
#send the query to server
response = sendRequest(sqlQuery);
#what is in response?
processResponse();
**** Response contains an Exception: "Query request too large.Suggestive row fetch 2000
rows.Total row fetch 30000" ****
#Declare two variables
long suggestiveRowFetch = 0; /*contains Suggestive RowFetch Count*/
long totalRowFetch = 0;      /*contains Total RowFetch*/
#fetch the two values and store it into variables.
parseExceptionMessage();
```

Testing Suggestions

This section provides tests that you can run to check various operations.

Testing ListPhoneByDescription and ListPhoneByName Methods

To test the ListPhoneByDescription and ListPhoneByName AXL methods, follow these steps:

Step 1 Populate database fields (<name>, <tkproduct>, <tkmodel>) for devices/phones to the maximum field size, which is 15 characters each.

Step 2 Populate the database with more than 60,000 devices.

Step 3 Execute the ListPhoneByDescription and ListPhoneByName AXL methods. The resulting data set has a response that is greater than 8 MB.

Expected Results: The interface returns "<API name> API request exceeds Threshold Limit. Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>." <API name> specifies the name of the API method.

Testing listDeviceByNameAndClass and listDeviceByServiceName Methods

To test the listDeviceByNameAndClass and listDeviceByServiceName AXL methods, follow these steps:

Step 1 Populate database fields (<name>, <tkproduct>, <tkmodel>) for devices/phones to the maximum field size, which is 15 characters each.

Step 2 Populate the database with more than 75,000 devices.

Step 3 Execute the listDeviceByNameAndClass and listDeviceByServiceName AXL methods. The resulting data set has a response that is greater than 8 MB.

Expected Results: The interface returns "<API name> API request exceeds Threshold Limit. Total rows matched: <Matched Rows>. Suggested row fetch: less than <Number of Rows>." <API name> specifies the name of the API method.

Testing the ExecuteSQLQuery AXL Method

To test the ExecuteSQLQuery AXL method, follow these steps:

Step 1 Populate database fields (<name>, <tkproduct>, <tkmodel>) for devices/phones to the maximum field size, which is 15 characters each.

Step 2 Create a SQL Select statement that retrieves this data.

Step 3 When the exception occurs, pick up the recommended Row Fetch Count and send the modified executeSQLQuery (in loop) by using the recommended row fetch count.

Expected Results: Demonstrate that Row Fetch Count logic works and, at the end loop, client can retrieve the entire set of required data from Cisco Unified Communications Manager.

Verifying That Tomcat Resources Are Protected

To verify that Tomcat resources are protected (Publisher server continues to operate under heavy AXL load):

Step 1 Write a script that generates a load on the AXL interface. Run executeSQLQuery to generate a response slightly less than 8 MB.

Step 2 Client runs this executeSQLQuery in a loop as soon as the transaction completes (both passed and failed transactions) for 1 hour. The client also notes the time that the request was sent, time that the response was received, and whether the response passed or failed.

Step 3 Create four instances of this script and make them run simultaneously against the same Cisco Unified Communications Manager Publisher.

Step 4 During the 1-hour load test, monitor the Tomcat JVM-related RTMT counters. In addition, use the Cisco Unified Communications Manager Administration interface to check whether you can list the devices on the system.

Step 5 At the end of the test, document the request and response times of the four clients on a timescale and note whether they succeeded or failed.

This analysis indicates whether the total responses that are processed by the AXL interface are within 16 MB. Every third concurrent request should have been rejected. By looking at the JVM on the Tomcat server that was available during the test, you can determine whether enough JVM exits to allow other applications to function properly.

Cisco Web Dialer API

The following sections describe updates to the Cisco Web Dialer API:

User Interface Enhancements

The following enhancements apply to the Make Call window:

- WebDialer Preferences moved to the Make Call window and show consolidated information.
- The MAC address displays only when a user is associated with multiple devices of the same type.
- Partition information does not display unless duplicate DNs are configured on the same device.
- The Calling Line option displays only when the device has multiple lines.
- The Extension Mobility option displays only when this feature is enabled for the user.

The following enhancements apply to the Hang Up window:

- The Destination User Name displays if it is available.
- Partition information does not display.

Hidden Proxy User Credentials

Credentials no longer display in clear text in a URL. For example, a URL that displayed as follows in previous versions

https://wdserver.com/webdialer/Webdialer?cmd=doSetProfile&destination=&loc=en-us&red=null&uid=wd&pwd=xyz

now displays as

https://wdserver.com/webdialer/Webdialer

As a result, developers who use the browser interface should use the HTTP POST method to pass the parameters. For example, this approach reduces the delay when Web Dialer converts GET parameters to POST:

```
<FORM action="https://42.88.86.1/webdialer/Webdialer" method="post">
    <P>
    <INPUT type="hidden" name="destination" value="+666">
```

```
    <INPUT type="submit" value="Send">
    </P>
</FORM>
```

Redirector Throttling

Redirector throttling supports up to 8 sessions/requests per second. The system throws the following error if it exceeds the throttle:

HTTP Status 503 - Service temporarily unavailable, please try again later

Configuration Changes

The following configuration changes occurred:

- List of Web Dialers setting displays on the Application server window in Cisco Unified Communications Manager Administration.
- Existing settings migrate automatically during an upgrade.
- No restriction exists on the number of Cisco Web Dialer servers that you can add.
- You can easily associate Cisco Web Dialers servers with Redirectors. To do so, take the following actions in the Application Server Configuration window in Cisco Unified Communications Manager Administration:
  1. In the Hostname or IP Address field, enter the host name or the IP address of the Cisco Web Dialer Server. Include the port number, if applicable.
  2. Assign the Cisco Web Dialer server to a particular Redirector Node. Choose Use None for a cluster-wide setting.

Update to Endcall SOAP Method

The SOAP method Endcall update means that it no longer drops all calls on a device. Endcall now ends an active call, but not a call on hold.

Internet Explorer 7 Support

When you exit Cisco Web Dialer when you run it with Internet Explorer 7, the pop-up window that prompts for confirmation no longer displays. This change does not affect the programming interface.

Cisco Unified IP Phones

This section provides the following information:

- Restrict Unconfigured Phone Registration, page 90
- Web Dialer Enhancements, page 91

See Table 9 for a listing of features and supported phone models.

Barge Tone Enhancements

The Party Entrance Tone configuration is available as a per-line setting, in *addition* to a service parameter setting for Cisco Unified CM administrators. The default value for the line setting specifies the service parameter setting. Because the Party Entrance Tone is configurable on a per-line basis, it is possible for one caller to hear a tone when he/she creates a conference, but if another caller has Party Entrance Tone set to No, then they do not hear the tone when that he/she creates another conference.

The Party Entrance Tone setting gets applied to Barge, cBarge, Join, Ad-hoc, and Meet Me conferences in the same manner as before.

Barge and cBarge support the interaction with Private Line Automatic Ringdown (PLAR). When a shared line has PLAR configured, a user can Barge or cBarge into a call that is connected on the shared PLAR line.

These Barge Tone enhancements gets supported on the following phones that are running SIP and SCCP:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

Busy Lamp Field (BLF) Enhancements

Cisco Unified Communications Manager 6.1(3x) introduces the following enhancements for the Busy Lamp Field (BLF) feature:

- New “BLF alerting” state—If configured, a new BLF line state, “BLF alerting,” notifies the monitoring phone user that the monitored line is in an Alerting state (ringing). An animated icon, LED appearance, and optional tone indicate BLF alerting.

- New BLF Pickup action—If BLF alerting is configured and a call is ringing on the monitored phone, the monitoring user can press the BLF pickup button to pick up the call.

These BLF enhancements get supported on the following phones that are running SCCP:

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

Where to Find More Information

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

Cisco Unified IP Phone Expansion Modules 7915 and 7916

The Cisco Unified IP Phone Expansion Module 7915 (grayscale display) and Cisco Unified IP Phone Expansion Module 7916 (color display) attach to your Cisco Unified IP Phone 7962G, 7965G, or 7975G (SCCP or SIP). Each expansion module adds up to 24 extra line appearances or programmable buttons to your phone. You can attach up to two expansion modules to your Cisco Unified IP Phone for a total of 48 extra line appearances or programmable buttons.

Note If the phone is running SCCP, you can only configure a maximum of 42 lines on your phone. For example, if you configure two 24-line Cisco Unified IP Phone Expansion Modules on a Cisco Unified IP Phone, only the first 42 lines will be available for use, including the first 6 or 8 lines on the Cisco Unified IP Phone.

Where to Find More Information

- *Cisco Unified IP Phone Expansion 7915 Phone Guide*
- *Cisco Unified IP Phone Expansion 7916 Phone Guide*

Cisco Unified IP Phone Support HTTPS

Cisco Unified IP Phones can securely access the web with the use of a phone trust store called "phone-trust." Administrators can upload certificates to a phone-trust store by using the Cisco Unified Communications Manager Operating System GUI. The Cisco Unified IP Phone will display a menu option called "Application Server" for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Cisco Unified IP Phone CTL file.

The phone-trust certificates and secure HTTPS web access get supported on the following phones that are running SCCP and SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Cisco Unified Communication Manager Security Guide*

Hold Status

Cisco Unified Communications Manager 6.1(3x) introduces the following enhancements to hold status:

- The Hold Status feature allows phones with a shared line to distinguish whether the local user placed the call on hold or a remote (shared line) user placed the call on hold.
- If two phone users share a line and one user places a call on hold, that user phone displays the local hold icon while the other user phone displays the remote hold icon. In addition, on the Cisco Unified IP Phone 7906G and 7911G, the hold button shows solid red on the local and remote phone. On all other supported phones, the local phone LED flashes green and the remote phone user LED flashes green.

The hold status enhancement gets supported on the following phones that are running SCCP and SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Line Select

Cisco Unified Communications Manager 6.1(3x) introduces settings to determine whether the primary line is automatically selected when a call is answered, or when the Messages button is pressed. Be aware that these settings can be made for all phones in the system, or for a single phone.

- **Line Select**: If this setting is disabled (default), the ringing line gets selected. When enabled, the primary line gets picked up even if a call is ringing on another line. The user must manually select the other line.
- **Line Select for Voice Messages**: When this setting is disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has a voice message, the first available line gets selected. When this setting is enabled, the primary line always gets used to retrieve voice messages.

Note Be aware that the primary line settings are also available for phones that are using extension mobility.

These enhancements are supported on the following SIP and SCCP phones:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G (SCCP only)

Where to Find More Information

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

Missed Calls

The missed calls feature allows the phone administrator to specify whether missed calls will get logged in the missed calls directory for a given line appearance. The following properties apply to the missed calls feature:

- The line can represent a directory number or shared line. The default behavior logs all missed calls on all lines.
- Missed call logging operates on a line basis. The line can represent a directory number or a shared line.
- If the phone administrator configures a line appearance (share or non-shared), so missed calls do not get logged, calls to that line never get logged in the missed call log directory, even if the calls eventually get forwarded due to no answer.
- If more than one line key gets configured on a phone, logging missed calls depends on the missed call log setting for each line.
- Missed call logging gets controlled by an on/off configuration parameter that is sent to the phone in the configuration file.
- The Missed Calls Log configuration does not affect any existing or previous call log items.
- Calls on lines that are not logged do not affect the New Missed Call status message.
- If the phone administrator turns off the missed calls feature on the configured line appearance, the missed calls do not get listed in the missed call history on that line appearance.

In addition to these properties, the following properties continue to apply all calls:

- All calls that are received on a phone appear in the Received Calls log, regardless of the line on which they were received.
- All calls that are made from a phone appear in the Placed Calls log, regardless of whether they were placed from a shared or primary line.

The missed calls feature gets supported on the following phones that are running SCCP and SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Personal Directory and Fast Dial Service

Administrators can set up a service URL that allows users to access their Fast Dials and PAB as services without having to authenticate each time:

- The administrator modifies a phone button template to associate a service URL and then assigns the phone button template to the user phone.
- In Cisco Unified CM User Options, the user assigns the service URL to an existing line button on the phone. The user can then press the line button to access the PAB or Fast Dials without having to authenticate.

The personal directory and fast dial service get supported on the following phones that are running SCCP and SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Restrict Unconfigured Phone Registration

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

With Cisco Unified Communications Manager 6.1(3x), if auto-registration is not enabled, and the phone has not been added to the Cisco Unified Communications Manager database, the phone will not attempt to register with Cisco Unified Communications Manager. The phone will continue to display the "Configuring IP" message until auto-registration has been enabled, or until the phone has been added to the Cisco Unified Communications Manager database.

The registration behavior is supported on the following phones and devices that are running SCCP and SIP:

  - Cisco Unified IP Phone 7906G
  - Cisco Unified IP Phone 7911G

- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G
- Cisco Analog Telephone Adapter
- VG248 Gateways

Where to Find More Information

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

Web Dialer Enhancements

Cisco Unified Communications Manager 6.1(3x) supports the following Web Dialer enhancements:

- Changing the WebDialer database location—The list of WebDialers moves from the Service Parameter Configuration window in Cisco Unified Communications Manager to be node-specific on the Application Server Configuration window. The Application Server Configuration window gets updated to enable sorting by application server type and node.
- Preferred Device menu name change—On the Cisco WebDialer Make Call window , the "Use permanent device" changes to display "Use preferred device." When only one preferred device is available, the MAC address will not display in the menu. MAC addresses will only display if two or more devices of the same type are assigned to the user.
- Merging the Preferences and Make Call windows together—The Cisco WebDialer Preferences window options are now available from the Cisco WebDialer Make Call window.
- Integration with Extension Mobility—If the user has an Extension Mobility profile, an option labeled "Use my Extension Mobility logged in device" will be available from the Preferred Device menu.
- Dialog changes for Hang-Up UI—Changes the text on the Hang-Up UI to say

  Calling <Username if available> at <dial-out number>

  If authorization codes are required, enter them now

The Web Dialer enhancements get supported on the following phones that are running SCCP and SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G

- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

Table 9 lists Cisco Unified IP Phones that support the Cisco Unified Communications Manager 6.1(3x) features.

Table 9 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1(3x) Features

Cisco Unified Communications Manager 6.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Barge Tone Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Barge Tone Enhancements, page 85
Busy Lamp Field (BLF) Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Busy Lamp Field (BLF) Enhancements, page 85
Cisco Unified IP Phone Expansion Modules 7915 and 7916	SCCP and SIP: 7962G 7965G 7975G	Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 86

Table 9 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1(3x) Features (continued)

Cisco Unified Communications Manager 6.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Cisco Unified IP Phone Support HTTPS	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Cisco Unified IP Phone Support HTTPS, page 86
Hold Status	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Hold Status, page 87

Table 9 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1(3x) Features (continued)

Cisco Unified Communications Manager 6.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Line Select	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Line Select, page 88
Missed Calls	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Missed Calls, page 89

Table 9 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1(3x) Features (continued)

Cisco Unified Communications Manager 6.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Personal Directory and Fast Dial Service	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Personal Directory and Fast Dial Service, page 90

Table 9 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1(3x) Features (continued)

Cisco Unified Communications Manager 6.1(3x) Feature	Cisco Unified IP Phone Support	For more information, see
Restrict Unconfigured Phone Registration	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Restrict Unconfigured Phone Registration, page 90
WebDialer Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Web Dialer Enhancements, page 91

Cisco Unified CM User Options

See the following sections for enhancements to the Cisco Unified CM User Options:

- Logging Missed Calls For Shared Lines, page 46
- Web Dialer Enhancements, page 91

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 6.1(3x) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Procedure

From http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs perform the following:

Step 1 In the Select Product Category list, double-click **Voice and Unified Communications**.

Step 2 In the Select Product list, double-click **Cisco Unified Communications Manager (CallManager)**.

Step 3 From the Version drop-down list, select the Unified CM version train for which you want to see defects (for example, for Unified CM Release 6.1(3x), select **6.1**.).

Step 4 Under Advanced Options, select **Use custom settings for severity, status, and others**.

Step 5 In the options that display, click the **Open** check box to deselect that option.

Now, the only option that will get acted upon is the **Fixed** option.

Step 6 Click **Search**.

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.

Using Bug Toolkit

Known problems (bugs) get graded according to severity level. These release notes contain descriptions of

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

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

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field; then, click **Go**.

For information about how to search for bugs, create saved searches, create bug groups, and so on, click **Help** in the Bug Toolkit window.

Open Caveats

The "Open Caveat as of February 12, 2009" section on page 100 describes possible unexpected behaviors, supported by component, in Cisco Unified Communications Manager Release 6.1(3x).

Tip For more information about an individual defect, click the associated Identifier in "Open Caveat as of February 12, 2009" section on page 100 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 Open Caveat as of February 12, 2009, page 100 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 98.

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.

Open Caveat as of February 12, 2009

The following list contains the caveat that was open on February 12, 2009.

Identifier: CSCsu54695

Component : media

Headline : IPVMS generates syslog messages.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Unified Communications Manager Release 6.1(1x) documentation suite was released.

Cisco Unified Communications Manager Administration Guide

The following sections comprise documentation updates for the *Cisco Unified Communications Manager Administration Guide*.

Incorrect Information Exists in the Meet-Me Number/Pattern Configuration

The Description field in the Meet-Me Number/Pattern Configuration Settings table incorrectly states that you can enter up to 30 alphanumeric characters as a description of the meet-me number/pattern.

The description should state that you can enter up to 50 characters in the description field.

Considerations for LDAP Port Configuration

Tip The following information does not display in the LDAP chapters in the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

When you configure the LDAP Port field in the LDAP Authentication window in Cisco Unified Communications Manager Administration, you specify the port number that the corporate directory uses to receive LDAP requests. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

Tip Your configuration may require that you enter a different port number than the numbers that are listed in the following bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

LDAP Port For When the LDAP Server Is Not a Global Catalog Server

- 389—When SSL is not required. (This port number is the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

LDAP Port For When the LDAP Server Is a Global Catalog Server

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Software Feature License

When you upgrade from any supported release of Cisco Unified Communications Manager to Release 6.1(3x), you must download and install a software feature license to activate the new features. The Cisco Unified Communication Administration Guide indicates that you must install a software feature license only if you are upgrading from 5.x or 6.x releases. You also need a license if you are upgrading from supported 4.x releases. For instructions about how to obtain and install a software feature license, see the "License File Upload" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Incorrect Description for User ID Field in Application User Window

The "Application User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can enter quotation marks (") in the User ID field in the Application User Configuration window in Cisco Unified Communications Manager Administration. In the User ID field, you can enter the following characters: alphanumeric (a-zA-Z0-9), dash(-), underscore(_), or space( ).

Logging In To the Web Interface When the Firewall Is Disabled

When the firewall is disabled, you must enter the URL of the Cisco Unified Communications Manager server in the following format to log in to the web interface:

https://*server***:8443/**

where *server* specifies the servername or IP address of the server.

Note Cisco does not recommend disabling the firewall.

Credential Policy Settings

The Credential Policy Configuration Settings (table) 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.

Deleting a Server

The *Cisco Unified Communications Manager Administration Guide* does not provide the messages that display when you attempt to delete a server. For information on these messages, see the "Deleting a Server and Adding a Deleted Server to a Cluster" section on page 12.

Disregard the entire section, Deleting a Server, in the "System-Level Configuration Settings" chapter in the *Cisco Unified Communications Manager System Guide*. Instead, see the "Deleting a Server and Adding a Deleted Server to a Cluster" section on page 12.

Unclear Documentation on Called Party Name Presentation

The *Cisco Unified Communications Manager Administration Guide* provides unclear information about called party name presentation.

The *Cisco Unified Communications System Guide* states that when the Always Display Original Dialed Number service parameter is set to True, the originating phone displays only the dialed digits for the duration of the call. To clarify the documentation, if you set the Cisco CallManager service parameter to True, the name of the called party does not display on the phone of the calling party.

The *Cisco Unified Communications Manager Administration Guide* does not state that setting the Always Display Original Dialed Number service parameter to True impacts the configuration for the Alerting Name field. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.

Misleading Documentation About Creating Cisco Unity and Cisco Unity Connection Voice Mailboxes

The *Cisco Unified Communications Manager Administration Guide* contains misleading information about creating Cisco Unity and Cisco Unity Connection voice mailboxes. Consider the following information when you configure the voice mailboxes:

- You can disregard the following statement in the *Cisco Unified Communications Manager Administration Guide*: "Ensure Cisco Unity Cisco Unified Communications Manager Integrated Voice Mailbox Configuration is enabled on the Cisco Unity or Cisco Unity Connection server."
- If you are integrating Cisco Unified Communications Manager 6.x with Cisco Unity Connection 2.x, you can use the import feature that is available in Cisco Unity Connection 2.x instead of performing the procedure that is described in the Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox section in the *Cisco Unified Communications Manager Administration Guide*. For information on how to use the import feature, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection 2.x*.

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.

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 portion in the 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 105.

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

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 the 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*.

Documentation Does Not Include the Latest List of Supported Phone Models

The *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Features and Services Guide* may not contain the latest list of supported Cisco Unified IP Phones. To identify whether the phone supports a feature, refer to the phone documentation that supports this version of Cisco Unified Communications Manager and the phone model.

Upgrade Procedure Contains Incorrect Information

In the Upgrading From Cisco Unified CallManager 4.x Releases section of the *Cisco Unified Communications Administration Guide*, the procedure indicates that a pop-up window displays when the user chooses an existing license file and chooses the **View File** button. The license actually displays in the main window after the screen refreshes

Application Server Configuration Not Required for Cisco Unity Connection 2.x

The *Cisco Unified Communications Manager Administration Guide* suggests that you must configure a Cisco Unity Connection 2.x server in the Application Server Configuration window in Cisco Unified Communications Manager Administration to maintain an association with the Cisco Unity Connection 2.x server. In fact, configuring a Cisco Unity Connection 2.x server in Cisco Unified Communications Manager Administration creates a blank list of user templates for Cisco Unity Connection in Cisco Unified Communications Manager. Instead of configuring the application server in Cisco Unified Communications Manager Administration, create an AXL connection via Unity Connection 2.x, as described in the System Administration Guide for Cisco Unity Connection. Creating the AXL connection via Cisco Unity Connection 2.x pushes a list of valid user templates for Cisco Unity Connection 2.x to Cisco Unified Communications Manager.

Incorrect Documentation on How to Delete Parameter for Phone Service

The Cisco Unified Communications Manager Administration Guide incorrectly states how to delete a service parameter in the IP Phone Services Configuration window in Cisco Unified Communications Manager Administration. To delete a parameter for an IP phone service, click the **Delete Parameter** button; after the deletion message displays, click **OK**.

To delete an IP phone service, click the **Delete** button in the IP Phone Services Configuration window or check the IP phone service check box in the Find and List Phone Services window and click **Delete Selected**.

Default Device Profile Chapter Incorrectly Includes Expansion Module Settings

The "Default Device Profile" chapter in the *Cisco Unified Communications Manager Administration Guide* includes descriptions for the following settings, which you cannot configure in the Default Device Profile Configuration window in Cisco Unified CM Administration: Module 1 and Module 2. Ignore these descriptions in this chapter.

Hunt Pilot Chapter Needs Clarification of Maximum Hunt Timer Setting

The "Hunt Pilot Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* provides the following description for the Maximum Hunt Timer setting:

Enter a value (in seconds) that specifies the maximum time for hunting. Valid values specify 1 to 3600. The default value specifies 1800 seconds (30 minutes).

This timer cancels if either a hunt member answers the call or if the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or hunting exhausts. If neither event takes place, hunting continues for 30 minutes, after which the call gets taken for final treatment.

Tip If hunting exceeds the number of hops that the Forward Maximum Hop Count service parameter specifies, hunting expires before the 30-minute maximum hunt timer value, and the caller receives a reorder tone.

In addition, the description should state that Cisco Unified CM only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.

Annunciator Chapter Contains Incorrect Information on Description Field

The "Annunciator Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* states that you can configure up to 54 characters in the Description field. Actually, you can configure up to 128 characters.

Gateway Configuration Chapter Contains Incorrect Information on Domain Name Field

The "Gateway Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can enter 50 characters in the Domain Name field in the MGCP gateway configuration window. Actually, you can enter up to 64 characters in the Domain Name field for MGCP gateways.

AAR Group Chapter Includes Incorrect Description for Dial Prefix Field

The "Automated Alternate Routing Group Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* includes incorrect entries for the Dial Prefix field.

Incorrect Information

Dial Prefix field—Enter the prefix characters and symbols to use for automated alternate routing within this AAR group. Valid entries include the following digits: [^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # . @

Correct Information

Dial Prefix field—Enter the prefix digits to use for automated alternate routing within this AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), and pound (#).

Dual Phone Mode Support

The "Cisco Unified IP Phone Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* omitted this information.

To support Mobile Connect and Mobile Voice Access for dual-mode phones, the following field displays on the Phone Configuration window:

Mobility User ID (dual-mode phones only) - From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned.

Note The Owner User ID and Mobility User ID can differ.

Generating a License File from DMA

The "License File Upload" chapter of the *Cisco Unified Communications Manager Administration Guide* for Release 6.1(3x) does not describe that there is an alternate method to obtain a product license. In this method, the user generates the product license from Data Migration Assistant (DMA). Data Migration Assistant User Guide Release 6.1(3x) describes how to use this method to generate the file.

Upgrading to Cisco Unified Communications Manager Release 6.1(3) from Cisco Unified Communications Manager 4.x Releases describes how to upload the file to Cisco Unified Communications Manager Release 6.1(3x).

Uploading a License File

The Uploading a License File section of the *Cisco Unified Communications Manager Administration Guide* does not instruct administrators to restart the Cisco CallManager service after uploading the license file. Administrators must restart the service for the license changes to take effect.

LDAP Authentication Chapter Omits Information on SSL Certificates and IP Addresses/Host Names

The "LDAP Authentication" chapter in the *Cisco Unified Communications Manager Administration Guide* does not contain the following information:

If you check the Use SSL check box in the LDAP Authentication window in Cisco Unified CM Administration, enter the IP address or the hostname that exists in the corporate directory SSL certificate in the Host Name or IP Address for Server field, which displays in the same window. If the certificate contains an IP address, enter the IP address. If the certificate contains the hostname, enter the hostname. If you do not enter the IP address or hostname exactly as it exists in the certificate, problems may occur for some applications; for example, applications that use CTIManager.

Tip You must upload the corporate directory SSL certificate into Cisco Unified CM by using the Cisco Unified Communications Operating System. For information on how to perform this task, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Enterprise Parameters and Service Parameters Chapters Omit Information on Set to Default Button

The "Enterprise Parameters Configuration" and the "Service Parameters Configuration" chapters in the *Cisco Unified Communications Manager Administration Guide* do not contain information on the Set to Default button. Clicking the Set to Default button in either the Enterprise Parameters Configuration window or Service Parameter Configuration window updates all parameters to the suggested value, which is the default that displays on the right side of the parameter. If a parameter does not have a suggested value, Cisco Unified CM does not update the value when you click the Set to Default button; for example, the Phone URL Parameters in the Enterprise Parameters Configuration window do not display a suggested value, so clicking the Set to Default button does not change the parameter that you configured.

A warning message displays after you click the Set to Default button. If you click OK in the dialog box, Cisco Unified CM updates all parameters in the configuration window to the suggested value; that is, if the parameter has a suggested value.

Information About Using an SRV Destination Port for the CUP Publish Trunk Service Parameter

The "Service Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* omits the following information.

You can configure a SIP trunk to use a DNS SRV port on a Cisco Unified Presenceserver as a destination. If you use a SIP trunk with a DNS SRV destination to configure the **CUP Publish Trunk** service parameter and then modify the DNS record, you must restart all devices (phones) that previously published, so they point to the correct Cisco Unified Presenceserver destination.

To configure the **CUP Publish Trunk** parameter, navigate to **System Service Parameters** and choose **Cisco CallManager** service for the server that you want to configure.

For an overview of configuring Cisco Unified Presence with Cisco Unified CM, see "Cisco Unified Communications Manager and Cisco Unified Presence High-Level Architecture Overview" in the *Cisco Unified Communications Manager System Guide*.

For SIP Trunks Used with Multiple Device Pools, Configure an SRV Destination Port

The "Trunk Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* omits the following information.

For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port.

From Cisco Unified CM Administration, choose **Device > Trunk**. Click **Find** to choose the SIP trunk that you want to edit or click **Add New** to create a new trunk.

When the Trunk Configuration window displays, enter the name of a DNS SRV port for the **Destination Address** and check the **Destination Address is an SRV Destination Port** check box.

Information About Changing Region Bandwidth Settings When Video Calls Are Made

The following informational reference will get added to the Cisco Unified Communications Manager administration documentation:

Refer to the "Regions" subtopic under the "Administration Considerations" topic of the "IP Video Telephony" chapter of the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

The reference will get added to the following topics of the Cisco Unified CM Administration documentation:

- document: *Cisco Unified Communications Manager Administration Guide*
  chapter: Location Configuration
  topic: list of restrictions at the beginning of the chapter
- document: *Cisco Unified Communications Manager Administration Guide*
  chapter: Region Configuration
  topic: list of limitations and restrictions at the beginning of the chapter

Information Omitted for Reroute Incoming Request to New Trunk Based on Setting

Instead of using the information for the Reroute Incoming Request to New Trunk Based on Setting in the "SIP Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*/online help, use the following information when you configure the Reroute Incoming Request to New Trunk Based on Setting in the SIP Profile Configuration window in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Cisco Unified Communications Manager accepts the call, Cisco Unified Communications Manager uses the configuration for this setting to determine whether the call should get rerouted to another trunk.

From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call gets rerouted:

- Never— If the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. Cisco Unified Communications Manager, which identifies the trunk by using the source IP address of the incoming packet and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived.
- Contact Info Header—If the SIP trunk uses a SIP proxy, choose this option. Cisco Unified Communications Manager parses the contact header in the incoming request and uses the IP address or domain name and signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If no SIP trunk is identified, the call occurs on the trunk on which the call arrived.
- Call-Info Header with purpose=x-cisco-origIP—If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Cisco Unified Communications Manager parses the Call-Info header, looks for the parameter, purpose=x-cisco-origIP, and uses the IP address or domain name and the signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If the parameter does not exist in the header or no SIP trunk is identified, the call occurs on the SIP trunk on which the call arrived.

Tip This setting does not work for SIP trunks that are connected to a Cisco Unified Presence proxy server or SIP trunks that are connected to originating gateways in different Cisco Unified CM groups.

Cisco Unified Communications Manager System Guide

The following sections comprise documentation updates for the *Cisco Unified Communications Manager System Guide*.

RSVP Reservation Teardown for Shared-Line Calls

The *Cisco Unified Communications Manager System Guide* incorrectly documents the teardown of RSVP reservations that takes place when a shared-line call gets answered. The RSVP and Shared-Line Calls section of the "Resource Reservation Protocol" chapter provides an example that includes the following erroneous statement to describe the reservation teardown:

After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 3, as well as the reservation between location 1 and location 4, get torn down.

The correct information follows:

After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 2, as well as the reservation between location 1 and location 4, get torn down. Only the RSVP reservation between location 1 and location 3 remains established.

Considerations for LDAP Port Configuration

Tip The following information does not display in the LDAP chapters in the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

When you configure the LDAP Port field in the LDAP Authentication window in Cisco Unified Communications Manager Administration, you specify the port number that the corporate directory uses to receive LDAP requests. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

Tip Your configuration may require that you enter a different port number than the numbers that are listed in the following bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

LDAP Port For When the LDAP Server Is Not a Global Catalog Server

- 389—When SSL is not required. (This port number is the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

LDAP Port For When the LDAP Server Is a Global Catalog Server

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

RSVP Reservation Teardown for Shared-Line Calls

The *Cisco Unified Communications Manager System Guide* incorrectly documents the teardown of RSVP reservations that takes place when a shared-line call gets answered. The RSVP and Shared-Line Calls section of the "Resource Reservation Protocol" chapter provides an example that includes the following erroneous statement to describe the reservation teardown:

After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 3, as well as the reservation between location 1 and location 4, get torn down.

The correct information follows:

After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 2, as well as the reservation between location 1 and location 4, get torn down. Only the RSVP reservation between location 1 and location 3 remains established.

Application Server Configuration Not Required for Cisco Unity Connection 2.x

The *Cisco Unified Communications Manager System Guide* suggests that you must configure a Cisco Unity Connection 2.x server in the Application Server Configuration window in Cisco Unified Communications Manager Administration to maintain an association with the Cisco Unity Connection 2.x server. In fact, configuring a Cisco Unity Connection 2.x server in Cisco Unified Communications Manager Administration creates a blank list of user templates for Cisco Unity Connection in Cisco Unified Communications Manager. Instead of configuring the application server in Cisco Unified Communications Manager Administration, create an AXL connection via Unity Connection 2.x, as described in the System Administration Guide for Cisco Unity Connection. Creating the AXL connection via Cisco Unity Connection 2.x pushes a list of valid user templates for Cisco Unity Connection 2.x to Cisco Unified Communications Manager.

Unclear Documentation on Called Party Name Presentation

The *Cisco Unified Communications Manager System Guide* provides unclear information about called party name presentation.

The *Cisco Unified Communications System Guide* states that when the Always Display Original Dialed Number service parameter is set to True, the originating phone displays only the dialed digits for the duration of the call. To clarify the documentation, if you set the Cisco CallManager service parameter to True, the name of the called party does not display on the phone of the calling party.

The *Cisco Unified Communications Manager Administration Guide* does not state that setting the Always Display Original Dialed Number service parameter to True impacts the configuration for the Alerting Name field. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.

Automated Alternate Routing (AAR) Limitation with Remote Gateways

AAR exhibits the limitation that calls that are routed over a remote gateway during a high-bandwidth situation fail, and the calls cannot be routed over the local gateway when AAR is used. This functionality proves to be important to customers who use Tail-End Hop Off (TEHO) for toll bypass.

Workaround Example

Use a specific partition for the TEHO in question.

In the following example, headquarters (HQ) has area code 408 and the Branch (BR1) has area code 919.

Configure as follows:

1. Create theTehoBr1forHQPt partition and assign this partition to the calling search space (CSS) of the HQ devices with a higher priority than the regular PSTN access uses.
2. Create the TehoBr1forHQRL route list and add the BR1 gateway route group to this route list as the first option and the HQ gateway as the second option.
3. Apply called party modification within the route list. In this case, apply predot called party modification for the BR1 route group, and apply predot and prefix 1919 called party modification for the HQ route group.
4. Ensure that the gateway does not perform called party modification.
5. Create a route pattern in the TehoBr1forHQPt partition.
6. Ensure that no called party modifications are applied in the route pattern.

Results

In an out-of-bandwidth situation, after Cisco Unified Communications Manager tries to allocate the first route group for TEHO (BR1 route group), Cisco Unified CM retries the second route group, at which point the system strips the 91919 string and replaces it with the 1919 string, which is suitable for long-distance dialing. Because the string is configured for use by the local gateway, less rerouting takes place.

AAR works on a per-external-phone-number-mask basis and cannot be processed for an external PSTN number because the system does not know the phone number mask of the PSTN number. This workaround provides AAR functionality and improves network resiliency.

Documentation Does Not State That Line Group With No Members Is Not Supported for Routing Calls

The Cisco Unified Communications Manager documentation does not state that you can configure an empty line group with no members (directory numbers) in Cisco Unified Communications Manager Administration. Although you can configure an empty line group with no members, Cisco Unified Communications Manager does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this situation, make sure that you configure at least one member in the line group.

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 the feature is 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.

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 exist 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.

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 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.

Tip Be aware that the enterprise parameter Denial-of-Service Protection Flag must be set to True for these parameter values to take effect.

Table 10 describes the configurable threshold values:

Table 10 SIP UDP Port Throttling Thresholds

Service Parameter	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 that is directed at the SIP station UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.
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 that is directed at the SIP trunk UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

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.

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 kb/s of available bandwidth, that link can support one G.711 call at 80 kb/s (in each direction), three G.723 or G.729 calls at 24 kb/s each (in each direction), or two GSM calls at 29 kb/s 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 kb/s of available bandwidth, that link can support two G.711 calls at 80 kb/s each, six G.723 or G.729 calls at 24 kb/s each, or five GSM calls at 29 kb/s 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

Directory Numbers Chapter Includes Incorrect Example for Shared Lines and Call Forward Busy Trigger

The "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide* includes incorrect example for shared lines and call forward busy trigger. Use the following information instead of the information in the guide:

Devices with shared-line appearance support the Call Forward Busy Trigger and the Maximum Number of Calls settings. You can configure Call Forward Busy Trigger per line appearance, but the configuration cannot exceed the maximum number call setting for that directory number.

The following example demonstrates how three Cisco Unified IP Phones with the same shared-line appearance, directory number 2000, use Call Forward Busy Trigger and Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

- Cisco Unified IP Phone 1—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 2—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 3—Configured a for maximum call value of 2 and busy trigger value of 2

When Cisco Unified IP Phone User 1 dials directory number 2000 for the first call, all three devices ring. The user for Cisco Unified IP Phone 3 picks up the call, and Cisco Unified IP Phones 1 and 2 go to remote in use. When the user for Cisco Unified IP Phone 3 puts the call on hold, user can retrieve the call from the Cisco Unified IP Phone 1 or Cisco Unified IP Phone 2. When User 2 dials directory number 2000 for the second call, only Cisco Unified IP Phone 3 rings.

Clustering Chapter Omits Information about Subsequent (Subscriber) Node

The "Clustering" chapter in the *Cisco Unified Communications Manager System Guide* does not state that Cisco Unified CM uses the subsequent (subscriber) node for database replication; that is, after you install Cisco Unified CM on the subsequent node, the node contains a replicate of the database that exists on the first node (publisher).

Tip To ensure that the subsequent node replicates the database of the first node, you must add the subsequent node to the Server Configuration window in Cisco Unified CM Administration on the first node before you install Cisco Unified CM on the server.

You can also use the subsequent node for call-processing redundancy and for load balancing. For information on how to configure call-processing redundancy and load balancing in Cisco Unified CM Administration, refer to the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Licensing Chapter Omits Information on Adjunct Licensing

The "Licensing" chapter in the *Cisco Unified Communications Manager System Guide* omits the fact that an error occurs when you configure an application, for example, Cisco IP Communicator, as the adjunct device, and the adjunct device requires more device license units (DLUs) than the primary device; for example, the Cisco Unified IP Phone 7906.

With adjunct licensing, fewer device license units (DLUs) get consumed for adjunct (secondary) devices, such as Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, when these applications get used with a Cisco Unified IP Phone 79xx, which serves as the primary device. For adjunct licensing to work, the adjunct device must consume fewer or the same number of DLUs as the primary device.

For example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7970, Cisco IP Communicator consumes only 1 DLU. Adjunct licensing works because the Cisco Unified IP Phone 7970 consumes 5 DLUs, and Cisco IP Communicator consumes 3 DLUs.

In another example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7906, adjunct licensing fails because the Cisco Unified IP Phone 7906 consumes 2 DLUs, and Cisco IP Communicator consumes 3 DLUs.

To ensure that Cisco Unified Communications Manager treats Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator as adjunct (secondary) devices, configure the Primary Phone setting in the Phone Configuration window for Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, as described in the "Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Cisco TFTP Chapter Omits Configuration Tip on Centralized TFTP

The "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the following information on configuring centralized TFTP:

For centralized TFTP configurations, ensure that the main TFTP server exists in the cluster that runs the highest version of Cisco Unified Communications Manager; for example, if you are using a centralized TFTP server between a compatible Cisco Unified CallManager 4.X cluster and a Cisco Unified Communications Manager 6.X cluster, ensure that your main TFTP server exists in the Cisco Unified Communications Manager 6.X cluster. If the main TFTP server exists in the cluster that runs the lower version of Cisco Unified Communications Manager, the phones use the locale files from the lower

version of Cisco Unified Communications Manager, which can cause issues with the phone; for example, the phone displays Undefined or ??? for the Do Not Disturb feature instead of displaying that DND is active. These errors display on the phone because the locale files that are served to the phones from the main cluster do not include the localized phrases.

Information About Changing Region Bandwidth Settings When Video Calls Are Made

The following informational reference will get added to the Cisco Unified Communications Manager administration documentation:

Refer to the Regions subtopic under the Administration Considerations topic of the "IP Video Telephony" chapter of the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

The reference will get added to the following topics of the Cisco Unified CM Administration documentation:

- document: *Cisco Unified Communications Manager System Guide*
  chapter: Understanding Video Telephony
  topic: Bandwidth Management
- document: *Cisco Unified Communications Manager System Guide*
  chapter: Call Admission Control
  topic: Bandwidth Calculations

Trunk Chapter Omits Restrictions for H.323/H.225 Trunks

The "Understanding Cisco Unified Communications Manager Trunks Types" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the following restriction for H.323/H.225 trunks.

You cannot configure more than one H.323 trunk of any type (gatekeeper- or non-gatekeeper-controlled) between the same clusters. Configuring more than one H.323 trunk can break inbound calls because Cisco Unified Communications Manager uses the received IP address to choose which trunk handles the call. If you configure more than one H.323 trunk between the same clusters, Cisco Unified Communications Manager may choose the wrong trunk device when a call gets processed. To avoid this issue, Cisco Unified Communications Manager checks the following configuration:

- Whether the remote Cisco Unified Communications Manager IP address that is configured for the trunk is the same as another remote Cisco Unified Communications Manager IP address for a configured trunk.
- Whether a remote Cisco Unified Communications Manager hostname for a configured trunk is the same as another remote Cisco Unified Communications Manager hostname for a configured trunk.

If you configure one trunk with an IP address, and you configure another trunk with a hostname that resolves to the same IP address, Cisco Unified Communications Manager does not detect this configuration, which causes duplicate trunk configuration and problems with call processing.

Cisco Unified Communications Manager cannot detect the configuration of a gatekeeper-controlled trunk and a non-gatekeeper-controlled trunk or the configuration of multiple gatekeeper-controlled trunks between the same Cisco Unified Communications Manager clusters. Additionally, Cisco Unified Communications Manager cannot detect the configuration of a gatekeeper-controlled H.323 trunk with

the configuration of an H.323 gateway that is accessible from that same gatekeeper-controlled H.323 trunk. These configurations can cause problems for call processing, so carefully configure your trunks in Cisco Unified Communications Manager to avoid these issues.

Voice-Messaging Chapters Omits Fact That Cisco Messaging Interface Service Parameters Must Be Configured Per Node

The voice-messaging chapters in the *Cisco Unified Communications Manager System Guide* do not state that you must configure the following Cisco Messaging Interface service parameters per node if you use the CMI service to deploy multiple third-party voice-messaging systems in the same Cisco Unified Communications Manager cluster.

- CallManager Name
- Backup CallManager Name
- Voice Mail DN
- Voice Mail Partition
- Alternate DN
- Alternate DN Partition

After you configure these parameters in the Service Parameters Configuration window, a message displays that warns that you must configure the value on each node in the cluster to achieve clusterwide support.

Information About Changing Region Bandwidth Settings When Video Calls Are Made

The following informational reference will get added to the Cisco Unified Communications Manager administration documentation:

Refer to the Regions subtopic under the Administration Considerations topic of the "IP Video Telephony" chapter of the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

The reference will get added to the following topics of the Cisco Unified CM Administration documentation:

- document: *Cisco Unified Communications Manager System Guide*
  chapter: Understanding Video Telephony
  topic: Bandwidth Management
- document: *Cisco Unified Communications Manager System Guide*
  chapter: Call Admission Control
  topic: Bandwidth Calculations

Cisco Unified Communications Manager Features and Services Guide

The following sections comprise documentation updates for the Cisco Unified Communications Manager Features and Services Guide.

- CTI and Attendant Console Chapters Omit Information on CTI Monitored Lines, page 120
- Incorrect Information on How to Install Assistant Console Application, page 120

CTI and Attendant Console Chapters Omit Information on 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

Incorrect Information on How to Install Assistant Console Application

The *Cisco Unified Communications Manager Features and Services Guide* incorrectly describes how to obtain the assistant console application for Cisco Unified Communications Manager Assistant. In release 6.1(1a), the assistant no longer obtains the assistant console application via the URL that is listed

in the guide. Instead, the assistant must download the Cisco Unified Communications Manager Assistant plug-in from Cisco Unified Communications Manager Administration (choose **Applications > Plugins**), as described in the "Cisco Unified Communications Manager Assistant User Guide" section on page 133.

The *Cisco Unified Communications Manager Features and Services Guide* does not state that the assistant console application supports Windows Vista.

Disregard the entire Assistant Console Dialog Options section in the *Cisco Unified Communications Manager Features and Services Guide*. Instead, use the information in the "Cisco Unified Communications Manager Assistant User Guide" section on page 133.

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.

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.

Devices Associated with the Attendant Console Application User

You 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.

CTI Devices Do Not Support Multicast Music on Hold (MOH)

CTI devices do not support the multicast Music on Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

Attendant Console Phones Do Not Support the Intercom Feature

The Cisco Unified Communications Manager Attendant Console does not support the intercom feature. The attendant console GUI shows intercom and other lines but does not display the hunt group member line when the intercom feature is configured on a phone that is a member of a hunt group.

Unclear Documentation on How Locales Work for Mobile Voice Access

The *Cisco Unified Communications Manager Features and Services Guide* does not address how locales work for mobile voice access. Mobile voice access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window in Cisco Unified Communications Manager Administration (**Media Resources > Mobile Voice Access**) when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.

Mobile Connect and Mobile Voice Access Chapter Omits Information About Configuring the Mobile Voice Access Media Resource

The "Mobile Connect and Mobile Voice Access" chapter in the *Cisco Unified Communications Manager Features and Services Guide* omits the following information about configuring the mobile voice access media resource:

Be aware that this configuration is required for making calls with the Mobile Voice Access feature. After the gateway collects the required digits from the user to make a call, the call gets transferred to the DN that is configured in this window. This DN can represent an internal DN to Cisco Unified Communications Manager, and the end user does not need to know the DN. The administrator must configure a dial-peer, so the MVA service can transfer the call from the gateway to this DN. Also, ensure this DN is placed in a partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN, as configured in the Inbound Calling Search Space for Remote Destination service parameter in the Clusterwide Parameters (System - Mobility) pane.

cBarge Chapter Omits Information on Shared Line Restriction for Conferences

The "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not contain the following cBarge restriction for shared lines and conferences:

If the number of shared-line users in the conference is equal to or greater than the configuration for the Maximum Number of Calls setting for the device from which you are attempting to barge, the phone displays the message, Error Past Limit.

Note The "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the previous information in the shared lines section.

Cisco Unified IP Phones Supporting Call Back with PLKs

The "Call Back" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information:

Many Cisco Unified IP Phone support the Cisco Call Back feature by using the programmable line key (PLK). 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

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.

Procedure

Step 1 From Cisco Unified Communications 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 6.1(1)*
- The “Intercom Directory Number Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.1(1)*
- The “Intercom Calling Search Space Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.1(1)*
- The “Intercom Partition Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.1(1)*
- The “Phone Button Template Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide Release 6.1(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.

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 6.1(1a). 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.)

None Option Not Documented for DND Incoming Call Alert Setting

The *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager Features and Services Guide* ("Do Not Disturb" chapter) do not describe the None option that displays in the DND Incoming Call Alert drop-down list box.

Tip The DND Incoming Call Alert drop-down list box displays in the Phone Configuration, Default Device Profile Configuration, and the Device Profile Configuration windows in Cisco Unified Communications Manager Administration.

The following information describes the DND Incoming Call Alert drop-down list box:

When you enable the DND Ringer Off option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options:

- None—For an incoming call, the device uses the settings that are defined in the common phone profile.
- Disable—This option disables both beep and flash notification of a call, but incoming call information still gets displayed.
- Beep Only—For an incoming call, this option causes the phone to play a beep tone only.
- Flash Only—For an incoming call, this option causes the phone to display a flash alert only.

Mobile Connect and Mobile Voice Access Chapter Contains Incorrect Information About Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

In the "Mobile Connect and Mobile Voice Access" chapter in the *Cisco Unified Communications Manager Features and Services Guide*, the procedure for configuring an H.323 gateway for system remote access by using hairpinning contains minor errors. The following procedure contains the corrected steps.

Procedure

Step 1 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later

- application service CCM

- http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12)

- call application voice Unified CCM
- http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

Step 2 Configure the dial-peer to associate mobile connect application with system remote access.

Sample configuration for IOS 12.3(13) and later

- dial-peer voice 1234567 voip
- service CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<*ip_address of call manager*>

Sample configuration for IOS 12.3(12) and earlier

- dial-peer voice 1234567 voip
- application CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<*ip_address of call manager*>

Step 3 Add a dial-peer for transferring calls to the Mobile Voice Access DN that is configured in the Configuring Mobile Voice Access Media Resources section of the "Mobile Connect and Mobile Voice Access" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Sample configuration for primary Cisco Communications Manager

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

Note This step specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

Note This step specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Step 4 Configure hairpin.

- voice service voip
- allow-connections h323 to h323

Mobile Connect and Mobile Voice Access Chapter Contains Incorrect Information About Configuring an H.323 Gateway for System Remote Access by Using PRI

In the "Mobile Connect and Mobile Voice Access" chapter in the *Cisco Unified Communications Manager Features and Services Guide*, the procedure for configuring an H.323 gateway for system remote access by using PRI contains minor errors. The following procedure contains the corrected steps.

Procedure

Step 1 Configure the T1/E1 controller for PRI from PSTN.

Sample configuration

- controller T1 1/0
- framing esf
- linecode b8zs
- pri-group timeslots 1-24

Step 2 Configure the serial interface for the PRI (T1/E1).

Sample configuration

- interface Serial 1/0:23
- ip address none
- logging event link-status none
- isdn switch-type primary 4ess
- isdn incoming-voice voice

- isdn bchan-number-order ascending
- no cdp enable

Step 3 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later

- application service CCM
- http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12)

- call application voice Unified CCM
- http://<Unified CM cluster Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

Step 4 Configure the dial peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later

- dial-peer voice 58888 pots
- service CCM *(Mobile Connect VXML application)*
- incoming called-number 58888
- no digit-strip

Sample configuration for IOS 12.3(12) and earlier

- dial-peer voice 100 pots
- application CCM *(Mobile Connect VXML application)*
- incoming called-number 58888 *(where* 58888 *represents the Mobile Voice Access number)*
- no digit-strip

Step 5 Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configured in the Configuring Mobile Voice Access Media Resources section of the Mobile Connect and Mobile Voice Access chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Sample configuration for primary Cisco Unified Communications Manager

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

Note This step specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric

- no vad

Sample configuration for secondary Cisco Unified Communications Manager (if needed)

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

Note This step specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Cisco Extension Mobility Chapter Error

The "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide* states that you can configure the Module 1 and Module 2 drop-down list boxes in the Default Device Profile Configuration window, which is not true.

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 6.1(1a).

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 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 the Barge with Shared Conference Bridge (cBarge) Configuration Checklist (table).

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.

Number of Alphanumeric Characters That Are 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.

Documentation Does Not Include the Latest List of Supported Phone Models

The *Cisco Unified Communications Manager Features and Services Guide* may not contain the latest list of supported Cisco Unified IP Phones. To identify whether the phone supports a feature, refer to the phone documentation that supports this version of Cisco Unified Communications Manager and the phone model.

Do Not Disturb Documentation Provides Incorrect Information About Phone Tone

The "Do Not Disturb" chapter in the *Cisco Unified Communications Manager Features and Services Guide* states that the phone periodically plays a tone to remind you that DND is active. The phone does not play a tone to remind you that DND is active. Instead, the status on the phone displays Do Not Disturb is active.

Destination Number in Remote Destination Configuration Window

The "Mobile Connect and Mobile Voice Access" chapter of the *Cisco Unified Communications Manager Features and Services Guide* incorrectly documents the Destination Number field of the Remote Destination Configuration window. In the Remote Destination Configuration Settings section, the following statements in the Destination Number description require correction:

- The maximum number of digits that are allowed in the Destination Number specifies 24, not 20 as stated.
- The current release does not support the digits A through D.
- This field supports the digits * (asterisk) and # (pound sign).

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 Manager Features and Services Guide*:

Original statement:

Some Cisco Unified IP Phones (such as 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 Call Back

The Interactions and Restrictions section in the "Cisco Call Back" chapter of the *Cisco Unified Communications Manager Features and Services Guide* did not get 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, refer to the phone administration guide that supports the phone and refer to the Telephony Features for the Cisco Unified IP Phone table.

To check which phones also support Cisco Call Back with PLKs, refer to the phone user guide that supports the phone and refer to the Understanding Feature Availability section.

Cisco Unified Communications Manager Security Guide

The following sections comprise documentation updates for the *Cisco Unified Communications Manager Security Guide*.

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.

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 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.

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.

Cisco Unified Communications Manager XML Developers Guide for Release 6.0(1)

The information in *Cisco Unified Communications Manager XML Developers Guide for Release 6.0(1)* applies to Release 6.1(1a), with the following updates:

- In the AXL Versioning Support section, the sample AXL request that carries version information now displays as follows:

```
POST /axl/ HTTP/1.0
Host:10.77.31.194:8443
Authorization: Basic Q0NNQWRtaW5pc3RyYXRvcjpjaXNjb19jaXNjbw==
Accept: text/*
Content-type: text/xml
SOAPAction: "CUCM:DB ver=6.1"
Content-length: 427
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body>
<axl:getUser xmlns:axl=http://www.cisco.com/AXL/API/6.1
xsi:schemaLocation="http://www.cisco.com/AXL/API/6.1
http://ccmserver/schema/axlsoap.xsd"
sequence="1234"> <userid>tttt</userid> </axl:getUser>
</SOAP-ENV:Body>
```

```
</SOAP-ENV:Envelope>
```

- In the AXL Versioning Support section, the sample AXL response now displays as follows:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONIDSSO=950805DE5E10F32C5788AE164EEC4955; Path=/
Set-Cookie: JSESSIONID=151CF94ACF20728B1D47CC5C3BECC401; Path=/axl; Secure
SOAPAction: "CUCM:DB ver=6.1"
Content-Type: text/xml;charset=utf-8
Content-Length: 728
Date: Mon, 22 Jan 2007 06:51:42 GMT
Connection: close
```

Cisco Unified Serviceability Administration Guide

The following sections comprise documentation updates for the *Cisco Unified Serviceability Administration Guide*.

DNS Required for RTMT Alerts by E-mail

The *Cisco Unified Serviceability Administration Guide* does not explain that to configure RTMT to send alerts via e-mail, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco Unified Communications Manager Server Configuration, see the "DHCP Server Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Warning Displays When SIP Stack Trace Is Enabled

In the Trace Configuration window in Cisco Unified Serviceability, Enable SIP Stack Trace represents one of the trace filter settings that are available. If you enable this log, you may experience severe performance degradation; so, when you click the Enable SIP Stack Trace check box, the following warning displays:

```
Enabling SIP Stack Trace can cause extreme performance degradation especially during high
traffic hours.
```

Missing MIB Changes

The *Cisco Unified Serviceability Administration Guide* requires updates for these MIB changes:

- Addition to Table 15-1 in the section Access Privileges (for V1 and V2): ReadNotifyOnly—The community string can read values of MIB objects and also send the values for trap and inform messages. To change the trap configuration parameters, you need to configure a community string with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.

- Addition to Table 16- 1 in the section Access Privileges (for V3): ReadNotifyOnly—The user can read values of MIB objects and also send the values for trap and inform messages. To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.

SNMP Traps and Informs Correction

The *Cisco Unified Serviceability Administration Guide* requires the deletion of this sentence from the SNMP Traps and Informs section: For some alarms, if the routing list in the alarm definition displays SNMP traps, the CCMAgent receives alarm notifications from the alarms. The notifications are received as XML messages which are parsed and traps are sent. In the case of Phone Failed and Phone Status events, the Phone Failed and Phone Status MMFs are populated.

Cisco Unified Communications Manager Assistant User Guide

The following sections comprise documentation updates for the *Cisco Unified Communications Manager Assistant User Guide*.

Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager 6.0

Consider the following note.

Note If the Assistant is configured with the Unified CM Intercom line, the speed dial on that line will initially point to the first Manager and then eventually to the last Manager that was called from the Intercom line.

Online Help Notes for Hebrew and Arabic

In the *Cisco Unified Communications Manager Assistant User Guide*, the chapter called "Introduction to Cisco Unified Communications Manager Assistant" does not contain the following information that Hebrew and Arabic users may need to know: Beginning in Cisco Unified Communications Manager Release 6.1 release, Cisco provides PDF versions of the *Cisco Unified Communications Manager Assistant User Guide* in Hebrew and Arabic as online help on the client PC that is running Cisco Unified Communications Manager Assistant. Therefore, this client must have Adobe Reader installed.

Cisco Unified Communications Manager Assistant

The assistant no longer obtains the assistant console application via a URL that the administrator provides; instead, a plug-in from Cisco Unified Communications Manager Administration gets downloaded and installed on the assistant PC.

The assistant console application installation supports Netscape 7.1 (or later) and Microsoft Internet Explorer 6 (or later). You can install the application on a PC that runs Windows 2000, Windows XP, or Windows Vista [new support for 5.1(3) and later].

A previous 5.x or 6.x version of the assistant console application works with Cisco Unified Communications Manager 6.1(1a), but if you decide to install the 6.1(1a) plug-in, you must uninstall the previous 5.x or 6.x version of the assistant console application before you install the plug-in.

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager 6.1(1a), you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

To uninstall previous versions of the assistant console application (6.0(1), 4.x, or any 5.x version before 5.1(3)), choose **Start> ...Programs > Cisco Unified CallManager Assistant > Uninstall Assistant Console**.

To uninstall 5.1(3) (or later) attendant console application, go to the Control Panel and remove it.

Tip The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified Communications Manager.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse into Cisco Unified Communications Manager Administration and choose **Application > Plugins**.

Step 2 For the Cisco Unified Communications Manager Assistant plug-in, click the **Download** link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click **Next**.

Step 5 Accept the license agreement and click **Next**.

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click **Next**.

Tip By default, the application installs in C:\Program Files\Cisco\ Unified Communications Manager Assistant Console.

Step 7 To install the application, click **Next**.

The installation begins.

Step 8 After the installation completes, click **Finish**.

Tip To launch the assistant console, click the desktop icon or choose **Cisco Unified Communications Manager Assistant > Assistant Console** in the Start...Programs menu.

Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Cisco Unified Communications Manager server where the Cisco IP Manager Assistant service is activated. The first time that the assistant logs in to the console, the assistant must enter the information in the Cisco Unified Communications Manager Assistant Server Port and the Cisco Unified Communications Manager Assistant Server Hostname or IP Address fields.

Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

The Advanced tab in the Cisco Unified Communications Manager Assistant Settings window allows you to enable trace for the assistant console.

Directory Search Correction

In the *Cisco Unified Communications Manager Assistant User Guide*, "Getting Started" chapter, the Using the Directory section, the following sentence exists:

To search for a coworker, enter any portion of the person's first and/or last name in the search fields and click Search. The directory displays a list of all users that match your search string.

Replace the preceding information with the following information:

To search in the directory, enter the first letter of the first name or the first letter of the last name, followed by the trailing letters in the first or last name (whichever name that you are entering), and click **Search**. The results that match the search string display.

The following wildcards do not get supported:

- *
- #
- +

Creating Filter Lists for a Manager

In the "How to Configure Manager Features" chapter of the *Cisco Unified Communications Manager Assistant User Guide*, in the How to Create Filter Lists for a Manager section, the following information now applies:

- Be aware that the + character is allowed in inclusive/exclusive filter configurations for managers via the browser-based configuration window for managers or the PC assistant console application. The + character signifies an international directory number that an end user may see (as a globalized number) in either the Cisco Unified Communications Manager directory or on the Cisco Unified IP Phone (under **Call Details > History**).
- The + character gets evaluated on an incoming call. For an incoming call to a manager, Cisco Unified Communications Manager Assistant will evaluate both localized and globalized numbers while performing filter pattern matching.

Cisco Unified IP Phone Documentation

The following sections comprise the documentation updates for the *Cisco Unified IP Phone Administration Guide*.

Cisco Unified IP Phone User Guide (7906, 7911, 7931, 7945, 7965, 7975)

The following information on extension mobility needs updating in the Cisco Unified IP Phone Guide (7906, 7911, 7931, 7945, 7965, 7975).

Using Cisco Extension Mobility

Cisco Extension Mobility (EM) allows you to temporarily configure a Cisco Unified IP Phone as your own. After you log in to EM, the phone adopts your user profile, including your phone lines, features, established services, and web-based settings. Your system administrator must configure EM for you.

Tips

- EM automatically logs you out after a certain time. Your system administrator establishes this time limit.
- Changes that you make to your EM profile from your User Options window take effect immediately if you are logged in to EM on the phone; otherwise, changes take effect the next time that you log in.
- Changes that you make to the phone from your User Options window take effect immediately if you are logged out of EM; otherwise, changes take effect after you log out.
- Local settings that are controlled by the phone do not get maintained in your EM profile.

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.

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.

Cisco Unified IP Phone Administration Guides (7905G, 7912G, 7921G)

The following information on Configuring a Custom Background Image needs updating in the Cisco Unified IP Phone Administration Guide (7905G, 7912G, 7921G).

Use the following procedure if you need to do the following types of updates to your IP phone:

- Change your logo, for which you will need the configuration file.
- Update your configuration file when the phone is in a locale other than "United States."

Tip For more information, see the Cisco Unified Communications Locale Installer 5.1.1.2000-1 Readme file.

Configuring a Custom Background Image

To configure custom background images for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Open a command window and enter the following command:

bmp2logo imageID image.bmp image.logo

where:

- imageID specifies a unique identifier for the new graphic. This identifier must comprise a number from 0 through 4294967296 and must differ from the identifier of the graphic that is currently on the phone.
- image specifies the base file name of the image that you previously created and saved with the graphics program.

Note The imageID of the image that comes with the phone specifies 1.

For example, if the image identifier is 10 and the base name of your image file is mylogo, enter this command:

bmp2logo 10 mylogo.bmp mylogo.log

Step 2 Copy the image.logo file to the following directory in the TFTP server for the Cisco Unified Communications Manager:

/usr/local/cm/tftp/<country>/

where:

<country> is the country of your locale installer (for example, Greece for Greek).

Note Be aware that the file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

Step 3 Add the following line to the Cisco Unified IP Phone profile file:

upgradelogo:imageID,TFTPServerID,image.logo

where:

- imageID specifies the same unique identifier that you specified in Step 1.

- TFTPServerID specifies the IP address of the TFTP server on which the image.logo file gets stored. If the image.logo file is stored on the same TFTP server as the Cisco Unified IP Phone configuration file, replace TFTPServerID with the numeral 0.
- image specifies the base file name of the image file.

For example, if the image identifier is 10, the converted file gets stored on the same TFTP server as the Cisco Unified IP Phone configuration file, and the base name of the converted image file specifies mylogo, add the following line to the configuration file:

upgradelogo:10,0,mylogo.logo

Note For detailed information about using profile files, see Appendix A, "Additional Configuration Methods and Parameters."

Step 4 Use the cfgfmt.exe tool to generate a binary profile file from the text file.

Step 5 Upload the new binary file that you created to the following directory in the TFTP server for the Cisco Unified Communications Manager:

//usr/local/cm/tftp/<lowercase country name>/

Note Be aware that the file name and directory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the directory path.

To upload the files, choose **Software Upgrades > Upload TFTP Server File** in Cisco Unified OS Administration.

For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

You must also copy the customized binary files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you also store backup copies of custom binary files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 6 Power cycle the phone.

The new graphic displays when the phone restarts.

Cisco Unified Wireless IP Phone Guide 7920 for Cisco Unified CallManager 5.0 (SCCP)

The Using Personal Directory on Your Phone section incorrectly states that you access the personal address book from the Services button on the Cisco Unified Wireless IP Phone 7920. The following section provides the correct procedure.

Using Personal Directory on Your Phone

The Personal Directory feature set contains your Personal Address Book (PAB) and Fast Dials. This section describes how to set up and use Personal Directory on your phone.

If you want to ...	Then ...
Access Personal Directory (for PAB and Fast Dial codes)	1. Choose **Menu > Directory > Corporate Directory > Personal Directory**. 2. Enter your Cisco Unified Communications Manager user ID and PIN; then, press **Submit**.

Cisco Unified Wireless IP Phone Guide (7975, 7971, 7965, 7945, 7962, 7942, 7941, 7931, 7911, 7906)

The information for Cisco Web Dialer for Cisco Unified Communications Manager 6.1(2) was updated in the *Cisco Unified IP Phone Guide for Cisco Unified Communications Manager 6.1(3)*.

Using Cisco Web Dialer

On the Preferences page (Make Call page in release 6.1(3x)), the default device for an Extension Mobility only user changed from Use EM Profile to Permanent Device. In release 6.1(3x), the default for EM only user changes back to Use EM Profile.

Cisco Unified CallManager Bulk Administration Guide

The following sections comprise documentation updates to the *Cisco Unified CallManager Bulk Administration Guide*.

Description for Phone Personalization Is Incorrect in Documentation

The *Cisco Unified Communications Manager Bulk Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Administration Guide* contain incorrect information on phone personalization. If you plan to configure the Phone Personalization setting in Cisco Unified Communications Manager Administration, use the following information:

The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. You can enable phone personalization in the Enterprise Parameter Configuration window, the Phone Configuration window, the Common Phone Profile Configuration window, or the Phone Template window in Cisco Unified Communications Manager Administration.

Tip To enable phone personalization via the Phone Personalization enterprise parameter, which supports all phones in the cluster that work with Phone Designer, choose **System > Enterprise Parameter** in Cisco Unified Communications Manager Administration, enter **1** in the Value Parameter field, and click **Save** in the Enterprise Parameter Configuration window.

If you configure phone personalization in the Phone Configuration window (Device > Phone), Common Phone Profile Configuration window (Device > Device Settings > Common Phone Profile), or the Phone Template window (Bulk Administration > Phones > Phone Template), choose one of the following options from the Phone Personalization drop-down list box:

- **Disabled**-The user cannot customize the Cisco Unified IP Phone by using Phone Designer.
- **Enabled**-The user can use Phone Designer to customize the phone.
- **Default**-The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window.

You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer release notes. To obtain the Phone Designer documentation, go to the following URL:

http://www.cisco.com/en/US/products/ps9829/tsd_products_support_series_home.html

Incorrect Path Is Documented for Add File Format Window

The "Phones and User File Format" chapter in the *Cisco Unified Communications Manager Bulk Administration Guide* includes an incorrect path to the Add File Format window. The Adding Phones/User File Formats section incorrectly states that you choose Bulk Administration > Phones and Users> Phones & Users File Format > Assign File Format to access the Add File Format window. Disregard the path in the BAT documentation and choose the following path to access the Add File Format window: **Bulk Administration > Phones and Users > Phones & Users File Format > Add File Format**.

Primary User Device Field on the Update Users Window in BAT

The *Cisco Unified CallManager Bulk Administration Guide* omitted this information. A new field called Primary User Device displays in the Mobility Information section of the End User Configuration window. This field controls the number of device license units that are consumed for adjunct devices for mobile connect and works in conjunction with the Enable Mobility check box in the End User Configuration window.You can access this window through **Users > Update Users**.

Single Button Barge (new field)—Phone Template Configuration Window in BAT

The *Cisco Unified CallManager Bulk Administration Guide* omitted this information. Single Button Barge (new field)—This new field displays in the Phone Template Configuration window, and when you add a new phone configuration for a phone that is running SCCP, a new row exists for Single Button

Barge/cBarge. You can set the Single Button Barge/cBarge feature Off, Barge. cBarge, or Default. If it is set to Default, the phone inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings.

Join Across Lines (new field)—Phone Template Configuration Window in BAT

The *Cisco Unified CallManager Bulk Administration Guide* omitted this information. Join Across Lines (new field)—This new field displays in the Phone Template Configuration window. When you add a new phone configuration for a phone that is running SCCP, a new row exists for Join Across Lines. You can set the Join Across Lines feature to Off, On, or Default. If it is set to Default, the phone inherits the Join Across Lines setting from the service parameter and device pool settings.

Single Button Barge (new field)—UDP Template configuration Window in BAT

The *Cisco Unified CallManager Bulk Administration Guide* omitted this information. Single Button Barge (new field)—This new field displays in the UDP Template configuration window. When you add a new device profile configuration for a phone that is running SCCP, a new row exists for Single Button Barge/cBarge. You can set the Single Button Barge/cBarge feature to Off, Barge, cBarge, or Default. If it is set to Default, the phone inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings.

Join Across Lines (new field)—UDP Template configuration Window in BAT

The *Cisco Unified CallManager Bulk Administration Guide* omitted this information. Join Across Lines (new field)—This new field displays inthe UDP Template configuration window. When you add a new device profile configuration for a phone that is running SCCP, a new row exists for Join Across Lines. You can set the Join Across Lines feature to Off, On, or Default. If it is set to Default, the phone inherits the Join Across Lines setting from the service parameter and device pool settings.

Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide

The following sections comprise the documentaiton updates for the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

- RTMT Trace and Log Central Disk IO and CPU Throttling, page 142
- Trace Compression Support, page 142
- Incorrect Description for User ID Field in Application User Window, page 103
- Path for Accessing Cisco Unified Reporting, page 143
- Perfmon Log File—Maximum File Size Default Value, page 143
- Path for Accessing Cisco Unified Reporting, page 143
- DNS Required for RTMT Alerts by E-mail, page 143
- Minimum Memory Requirement for RTMT Client, page 143

RTMT Trace and Log Central Disk IO and CPU Throttling

RTMT now supports the throttling of critical Trace and Log Central operations and jobs, whether they are running on demand, scheduled, or automatic. The throttling slows down the operations when IO utilization is in high demand for call processing, so call processing can take precedence.

When a user makes a request for an on-demand operation when the call processing node is running under high IO conditions, the system now displays a warning, which gives the user the opportunity to abort the operation. You can configure the IO rate threshold values that control when the warning displays with the following new service parameters:

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The system compares the values of these parameters against the system actual CPU and IOWait values. If the goal (the value of the service parameter) is lower than the actual value, the system issues the warning.

For More Information

- "Service Parameters Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*

Trace Compression Support

The following information provides an updated version of what appears in the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

This feature enables the ROS (Recoverable Outstream) library to support the compressed output of tracefiles. The files get compressed as they are being generated. The benefits of tracefile compression include

- Reduces the capacity required to store tracefiles.
- Reduces the disk head movement, which results in significantly improved disk I/O wait. This may prove to be of value when tracefile demand is high.

Use the new enterprise parameter, Trace Compression, to enable or disable trace compression. The default value for this parameter specifies Disabled. For information on setting the values of enterprise parameters, see the "Enterprise Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Caution Compressing files adds additional CPU cycles. Enabling the Trace Compression enterprise parameter can negatively impact overall call throughput by as much as 10 percent.

You can recognize compressed files by their .gz extension (.gzo if the file is still being written to). To open a compressed file, double click the file name, and the file opens in the log viewer.

For More Information

- "Enterprise Parameters Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*

Path for Accessing Cisco Unified Reporting

In both the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* ("Installing and Configuring Real-Time Monitoring Tool" chapter) and the *Cisco Unified Serviceability Administration Guide* ("Understanding Cisco Unified Serviceability" chapter), the RTMT menu path for accessing Cisco Unified Reporting is incorrect. The correct path follows: **File>Cisco Unified Reporting**.

Perfmon Log File—Maximum File Size Default Value

Chapters 4 and 5 ("Understanding Performance Monitoring" and "Configuring and Displaying Performance Counters") in the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* incorrectly specify the default value of the Maximum File Size perfmon data-logging parameter as 2 megabytes. The correct default value equals 5 megabytes.

Path for Accessing Cisco Unified Reporting

Both the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* ("Installing and Configuring Real-Time Monitoring Tool" chapter) and the *Cisco Unified Serviceability Administration Guide* ("Understanding Cisco Unified Serviceability" chapter) show an incorrect RTMT menu path for accessing Cisco Unified Reporting. The correct path follows: **File>Cisco Unified Reporting**.

DNS Required for RTMT Alerts by E-mail

The *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* do not explain that to configure RTMT to send alerts via Email, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco Unified Communications Manager Server Configuration, see the "DHCP Server Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Minimum Memory Requirement for RTMT Client

Chapter 2, "Installing and Configuring Real-Time Monitoring Tool (RTMT)" in the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* does not include the minimum memory requirement for running the RTMT client on a Windows OS machine. The minimum memory requirement equals 128 MB.

Cisco Unified Communications Operating System Administration Guide

The following sections comprise documentation updates for the *Cisco Unified Communications Operating System Administration Guide*.

Support for NIC Teaming

The *Cisco Unified Communications Operating System Administration Guide* does not indicate the appropriate support for NIC teaming. Server platforms with dual Ethernet network interface cards (NICs) can support NIC teaming for network fault tolerance with Cisco Unified Communications Manager . Cisco began support of NIC teaming on HP servers in the 5.0(1) release and began support on IBM servers in the 6.1(2) release. This feature allows a server to be connected to the Ethernet via two NICs and, hence, two cables. NIC teaming prevents network downtime by transferring the workload from the failed port to the working port. NIC teaming cannot be used for load balancing or increasing the interface speed.

Install New COP Files Before You Upgrade Cisco Unified Communications Manager

If you have new .cop files for your devices, be sure you install them before you upgrade Cisco Unified Communications Manager to a newer build. If you do not install the new .cop file before you upgrade, your devices might not function correctly after the upgrade.

Digital Certificate Key Length Restrictions

In 5.x releases of Cisco Unified Communications Manager you must use digital certificates with a key length of 2048 bits or less. Cisco Unified Communications Operating System in these releases does not support digital certificates with a key length larger than 2048 bits.

Parallel Upgrades from Unified CM Releases 5.x and 6.x to Unified CM Release 6.1(3x)

When you upgrade a cluster that is running a supported version of Cisco Unified Communications Manager 5.x or 6.x to Cisco Unified Communications Manager 6.1(3x), begin upgrading the first node first. You can begin upgrading subsequent nodes in parallel after the first node has reached a specified point in the upgrade.

During the upgrade of the first node, view the installation log, install_log_<date+time>.log, by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or the command line interface (CLI). You can begin the upgrade of the subsequent nodes after the following information displays in the log.

PRODUCT_TARGET is <product target id>

PRODUCT_NAME is <product name>

PRODUCT_VERSION is <product version to which you are upgrading, such as 6.1(2)>

You can also use the CLI to search for the relevant information in the install log by following this procedure:

Procedure

Step 1 List the install logs; for example:

```
file list install install_* date

install_log_2008-10-01.09.41.57.log     install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

Step 2 Search the most recent install log for the string PRODUCT_VERSION; for example:

```
file search install install_log_2008-10-14.09.31.06.log PRODUCT_VERSION

Searching path: /var/log/install/install_log_2008-10-14.09.31.06.log
Searching file: /var/log/install/install_log_2008-10-14.09.31.06.log
10/14/2008 09:52:14 upgrade_os.sh|PRODUCT_VERSION is 7.1.0.39000-97|<LVL::Info>

Search completed
```

Step 3 When the **file search** command finds the PRODUCT_VERSION string in the install log, you can start the upgrade of the subsequent nodes.

Caution If you want to upgrade the subsequent nodes in parallel with the first node, do not choose the Reboot to upgraded partition on either first node or subsequent nodes while you are configuring the upgrade options. If selected, the first node may complete its upgrade and reboot while the subsequent nodes are upgrading, which causes the upgrade of the subsequent nodes to fail.

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

Remote Support Account Duration

When you create a remote support account in Cisco Unified Communications Operating System Administration, you must enter the duration for which the account will be active in the **Account Duration** field. Enter a number of days between 1 and 30. The remote support account will automatically expire after the number of days that you enter. The default account duration specifies 30 days.

System Generates a DBReplicationFailure Alert

During supported upgrades from Cisco Unified Communications Manager 5.x or 6.x to Cisco Unified Communications Manager 6.1(x), the system may generate a DBReplicationFailure alert while the system transitions to the new software release. Administrators can disregard this alert until all servers in the cluster have been upgraded and are running Cisco Unified Communications Manager 6.1(x).

For more information on viewing alerts, refer to the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

Information On ARP Cache Limits Omitted from Operating System Administration Guide

Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.

Third-Party Certificate Authority Verification

The *Cisco Unified Communications Operating System Administration Guide*, Release 6.0(1) states that Cisco has verified Verisign as a source for third party certificates. Be aware that this is no longer correct, and Verisign is not a verified CA.

Recovering Administrator and Security Passwords

This section replaces the section Recovering the Administrator Password in the "Log In to Cisco Unified Communications Operating System Administration" chapter" of the *Cisco Unified Communications Operating System Administration Guide* for releases 5.0(4), 5.1(1), 6.0(1), and 6.1(1a).

If you lose the administrator password or security password, use the following procedure to reset these passwords.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 To continue, press any key.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- To reset the administrator password, enter **a**.
- To reset the security password, enter **s**.
- To quit, enter **q**.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

Caution The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Software Feature License Information Omitted from Operating System Administration Guide

The "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide* omits the following information:

You must obtain a software feature license if you are upgrading from Cisco Unified Communications Manager 5.x. A software feature license activates features on your system for the specified license version. To use 5.0 device licenses with Cisco Unified Communications Manager 6.(x) or later, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.

For more information on obtaining and installing licenses, see the "License File Upload" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Cisco Unified Communications Manager Does Not Support Recovery of Administration or Security Passwords

Chapter 2 of the *Cisco Unified Communications Operating System Administration Guide* does not contain the following information.

Cisco Unified CM does not support recovery of administration or security passwords. If you lose these passwords, you must reset the passwords, as described in the *Cisco Unified Communications Operating System Administration Guide*.

Tip The *Cisco Unified Communications Operating System Administration Guide* calls the section Recovering the Administrator or Security Passwords, instead of Resetting the Administrator or Security Passwords. Access the Recovering the Administrator or Security Passwords section to reset the passwords.

Characters Allowed in a Pre-Shared Key

Chapter 6 of the *Cisco Unified Communications Operating System Administration Guide* does not contain the following information.

Pre-shared IPSec keys can contain alphanumeric characters and hyphens only, not white spaces or any other characters. If you are migrating from a Windows-based version of Cisco Unified CM, you may need to change the name of your pre-shared IPSec keys, so they are compatible with current versions of Cisco Unified CM.

Troubleshooting Guide for Cisco Unified Communications Manager

The following section comprises documentation updates for the *Troubleshooting Guide.*

Automated Alternate Routing (AAR) Limitation with Remote Gateways

AAR exhibits the limitation that calls routed over a remote gateway during a high-bandwidth situation fail, and the calls cannot get routed over the local gateway when AAR is used. Be aware that this functionality is important to customers who use Tail-End Hop Off (TEHO) for toll bypass.

Workaround Example

Use a specific partition for the TEHO in question.

In the following example, headquarters (HQ) has area code 408, and the Branch (BR1) has area code 919.

Configure as follows:

1. Create theTehoBr1forHQPt partition and assign this partition to the calling search space (CSS) of the HQ devices with a higher priority than the regular PSTN access uses.
2. Create the TehoBr1forHQRL route list and add the BR1 gateway route group to this route list as the first option and the HQ gateway as the second option.
3. Apply called party modification within the route list. In this case, apply predot called party modification for the BR1 route group, and apply predot and prefix 1919 called party modification for the HQ route group.
4. Ensure that the gateway does not perform called party modification.
5. Create a route pattern in the TehoBr1forHQPt partition.
6. Ensure that no called party modifications are applied in the route pattern.

Results

In an out-of-bandwidth situation, after Cisco Unified Communications Manager tries to allocate the first route group for TEHO (BR1 route group), Cisco Unified CM retries the second route group, at which point the system strips the 91919 string and replaces it with the 1919 string, which is suitable for long-distance dialing. Because the string is configured for use by the local gateway, less rerouting takes place.

AAR works on a per-external-phone-number-mask basis and cannot be processed for an external PSTN number because the system does not know the phone number mask of the PSTN number. This workaround provides AAR functionality and improves network resiliency.

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone

Symptom

When a remote destination (mobile phone) is not a smart phone and a call to this mobile phone is anchored through Cisco Unified CM, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

Possible Cause

If the calling party receives busy/reorder/disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. Cisco Unified CM cannot recognize this circumstance because no disconnect signals came from the provider. To verify whether this is the case, let the calling party wait for 45 seconds, when service provider will time out and send disconnect signals, upon which Cisco Unified CM can provide a **Resume** softkey to resume the call.

Recommended Action

Perform the following actions:

- Add the following command to the gateway:

  voice call disc-pi-off

- For the Cisco CallManager service, set the Retain Media on Disconnect with PI for Active Call service parameter to False.

Netdump Utility

The netdump utility allows you to send data and memory crash dump logs from one server on the network to another. Servers that are configured as netdump clients send the crash logs to the server that is configured as the netdump server. The log file gets sent to the crash directory of the netdump server.

In a Cisco Unified Communications Manager cluster, you must configure at least two nodes as netdump servers, so the first node and subsequent nodes can send crash dump longs to each other.

For example, if your cluster contains three servers (one primary/first node and two subsequent nodes), you can configure the first node and subsequent node #1 as the netdump servers. Then, you can configure the first node as a netdump client of the subsequent node #1 and configure all of the subsequent nodes as netdump clients of the first node. If the first node crashes, it sends the netdump to subsequent node #1. If any subsequent node crashes, it sends the netdump to the first node.

You can use an external netdump server rather than configuring a Cisco Unified Communications Manager server as a netdump server. For information on configuring an external netdump server, contact TAC.

Note Cisco recommends that you configure the netdump utility after you install Cisco Unified Communications Manager to assist in troubleshooting. If you have not already done so, configure the netdump utility before you upgrade Cisco Unified Communications Manager from supported appliance releases.

To configure the netdump servers and clients, use the command line interface (CLI) that is available for the Cisco Unified Communications Operating System as described in the following sections:

- Configuring a Netdump Server, page 151
- Configuring a Netdump Client, page 151
- Working with Files That Are Collected by the Netdump Server, page 151
- Monitoring Netdump Status, page 152

Configuring a Netdump Server

To configure a node as a netdump server, use the following procedure:

Procedure

Step 1 On the node that you want to configure as the netdump server, start a CLI session as described in the *Cisco Unified Communications Operating System Administration Guide*.

Step 2 Execute the **utils netdump server start** command.

Step 3 To view the status of the netdump server, execute the **utils netdump server status** command.

Step 4 Configure the netdump clients, as described in the "Configuring a Netdump Client" section on page 151.

Configuring a Netdump Client

To configure a node as a netdump client, use the following procedure:

Procedure

Step 1 On the node that you want to configure as the netdump client, start a CLI session as described in the *Cisco Unified Communications Operating System Administration Guide*.

Step 2 Execute the **utils netdump client start** *ip-address-of-netdump-server* command.

Step 3 Execute the **utils netdump server add-client** *ip-address-of-netdump-client*. Repeat this command for each node that you want to configure as a netdump client.

Note Make sure that you enter the correct IP addresses. The CLI does not validate the IP addresses.

Step 4 To view the status of the netdump client, execute the **utils netdump client status** command.

Working with Files That Are Collected by the Netdump Server

To view the crash information from the netdump server, use the Real-Time Monitoring Tool or the command line interface (CLI). To collect the netdump logs by using the Real-Time Monitoring Tool, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Netdump logs check box. For more information on collecting files by using Real-Time Monitoring Tool, see the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the netdump logs, use the "file" CLI commands on the files in the crash directory. The log filenames begin with the IP address of the netdump client and end with the date that the file gets created. For information on the file commands, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Monitoring Netdump Status

You can monitor the netdump status by configuring SyslogSearchStringFound alerts in the Real-Time Monitoring Tool. Use the following procedure to configure the appropriate alerts:

Procedure

Step 1 From the quick launch channel in Real-Time Monitoring Tool, choose **Tools > Alert Central**.

Step 2 Right-click the SyslogStringMatchFound alert and choose **Set Alert/Properties**.

Step 3 Click **Next** three times.

Step 4 On the SysLog Alert window, click the **Add** button. When the Add Search String dialog box displays, enter **netdump: failed** and click **Add**. Then, click **Next**.

Note Make sure that the case and syntax match exactly.

Step 5 On the Email Notification window, choose the appropriate trigger alert action, enter any user-defined e-mail text, and click **Save**.

Cisco Unified Communications Manager 6.1 TCP and UDP Port Usage

The following section comprises the documentation updates for the *Cisco Unified Communications Manager 6.1 TCP and UDP Port Usage* documentation.

Ephemeral Port Range

The Cisco Unified Communications Manager 6.1 TCP and UDP Port Usage document requires the following update:

The Ephemeral port range for the system equals 32768 - 61000.

Obtaining Documentation and Submitting a Service Request

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

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

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