Release Notes for Cisco Unified Communications Manager Release 6.1(1b)

June 10, 2008

This document contains information that existed in the Cisco Unified Communications Manager Releases 6.1(1), 6.1(1a) and the "For Release 6.1(1b)" information indicated in Table 1.

.

Table 1 Updated Information

Date	Change
June 20, 2008	Under Documentation Updates > Updates, added the " Updated List of Fields Supported for Export by the Import/Export Tool" section on page 96.
June 10, 2008	Under New and Changed Information, added the " Basic Uninterruptible Power Supply (UPS) Integration" section on page 16.
April 14, 2008	**For Release 6.1(1b)** • Under Important Notes, added " Installation Note" section on page 9 • Under Important Notes added " Cisco Recommendations" section on page 8 • Updated the " Summary of Cisco Unified Communications Manager Release 6.1(1b)" section on page 2 • Updated the "Table 8 Open Caveats as of April 7, 2008" section on page 78 • Updated the " Upgrading from Cisco Unified Communications Manager Release 6.0(1a) or 6.1(1a) to Release 6.1(1b) Using the UCSInstall File" section on page 6 • Added the " CAR Records Migration Issues" section on page 82 • Added the " Summary of Cisco Unified Communications Manager Release 6.1(1b)" section on page 2

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

Table 1 Updated Information

Date	Change
February 5th through February 13th, 2008	**For Release 6.1(1a):** • Under Important Notes, added the " Out of Service Nodes and Cisco License Manager" section on page 9 • Under Documentation Updates > Updates, added the " Missing MIB Changes" section on page 97 and the " SNMP Traps and Informs Correction" section on page 97. • Under New and Changed Information, added the " Disaster Recovery Manual Backup Window" section on page 18 • Under Documentation Updates > Omissions, added " Disaster Recovery Manual Backup Checkbox" section on page 82 • Under New and Changed Information, added the " New Service Parameters Added to Extension Mobility" section on page 17 • Added the " • CSCsm15075 In 6.1(1), when you click the Find button an Access Denied error got generated on systems with more than 250 gateways and/or route lists provisioned. In 6.1(1a) permissions were changed to allow the Find and List window to be loaded from the Route Pattern window." section on page 3

These release notes describe the caveats that release 6.1(1a) and 6.1(1b) resolve as well as the new features and caveats for Cisco Unified Communications Manager Release 6.1(1x). 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

Summary of Cisco Unified Communications Manager Release 6.1(1b)

The following noncomprehensive list gives the caveats that were resolved in this release of Unified CM:

1. CSCsm37017 - Prior to this release, when you configured traces in the serviceability window, no CCMUser option existed, which meant that you could not change the default CCMuser trace level.
2. CSCso11097 - Prior to this release, when you upgraded from Release 6.0 to 6.1, a corruption of the RAID controller firmware on a MCS-7845-I2 server existed. After the reboot that the upgrade required, the restart failed with an error:

   "ATTENTION: The Firmware image in the controller is corrupted!! Please run the Firmware Update Utility from the OS to update the firmware. Error code: 86"
3. CSCso53771 - According to Cisco Security, several products in the Cisco Unified Communications family of products contained a command execution vulnerability in the Disaster Recovery Framework (DRF) feature. A remote, unauthenticated user could exploit this vulnerability to execute arbitrary commands that may allow full administrative access to affected systems.
4. CSCso45910 - Prior to this release, after an upgrade, the server would not boot to the new partition.
5. CSCsm47603 - Prior to this release, the BIOS that is bundled with Release 6.1 did not support the E6400 processor that IBM put into their 7825I3 servers, and the BIOS got downrevved to the unsupported version during install/upgrade.

6. CSCsl31392 - Prior to this release, in DMA messages intended to identify problems in the user data could be misinterpreted as logging errors. Even if the user correctly identified the problem, the required user action was not evident. Release 6.1(1b) includes expanded explanations for five additional error cases DMA. The resulting user visible error messages provide a better understanding of cause and resolution.

- CSCsm15075 In 6.1(1), when you click the **Find** button an Access Denied error got generated on systems with more than 250 gateways and/or route lists provisioned. In 6.1(1a) permissions were changed to allow the Find and List window to be loaded from the Route Pattern window.

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the " Important Notes" section on page 7 for information about issues that may affect your system.

Note To ensure continuous operation and optimal performance of your Cisco Unified Communications Manager system, you must upgrade to Cisco Unified Communications Manager 6.1(1a).

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the " Upgrading System Software" section on page 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(1b) 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(1b), 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(1b).

Note Some servers that are listed in the compatibility matrix may require additional hardware support for Cisco Unified Communications Manager Release 6.1(1b). 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(1b), 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(1b), 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.

Upgrading System Software

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(1b)

It is possible to upgrade directly to Cisco Unified Communications Manager 6.1(1b) from:

- 4.1(3x)
- 4.2(3x)
- 5.1(1x)
- 5.1(2x)
- 5.1(3x)
- 6.0(1x)
- 6.1(1x)

Caution Use the iso files mentioned in the " Upgrading from Cisco Unified Communications Manager Release 6.0(1a) or 6.1(1a) to Release 6.1(1b) Using the UCSInstall File" section on page 6 for upgrades from 6.0(1a) or 6.1(1a) to 6.1(1b) only.

Upgrading from CUCM 4.x and 5.x

If you are upgrading from 4.1.3, 4.2.3, 5.1.1, 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 are required to enter your Cisco Software Application Support Plus Upgrades (SASU) contract number and request the CD/CD set. If you do not have a SASU contract, 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 Cisco Unified Communications Manager Release 6.0(1a) or 6.1(1a) to Release 6.1(1b) Using the UCSInstall File

Caution Do not use the following information to upgrade from any Unified CM release other than 6.0(1a) or 6.1(1a).

Because of its size, the UCSInstall iso file, UCSInstall_UCOS_6.1.1.2000-3.sgn.iso, has been divided into two parts:

- UCSInstall_UCOS_6.1.1.3000-2.sgn.iso_part1of2
  - MD5 value specifies 1e47a96d3b89b8e1dfcefef3e8cdaa3a
- UCSInstall_UCOS_6.1.1.3000-2.sgn.iso_part2of2
  - MD5 value specified 885c93ae61d75978646ced37d25a791a)

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 6.1.1.3000-2 build is a non-bootable ISO which is only useful for upgrades. It cannot be used 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_6.1.1.3000-2.sgn.iso_part1of2 UCSInstall_UCOS_6.1.1.3000-2.sgn.iso_part2of2 > UCSInstall_UCOS_6.1.1.3000-2.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_6.1.1.3000-2.sgn.iso_part1of2+UCSInstall_UCOS_6.1.1.3000-2.sgn.iso_part2of2 UCSInstall_UCOS_6.1.1.3000-2.sgn.iso
```

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

38ea200efd06fb6bb8c0515fd852aadb UCSInstall_UCOS_6.1.1.3000-2.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(1a)	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(1a). 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(1x).

- Installation Note, page 9
- Cisco Recommendations, page 8
- Out of Service Nodes and Cisco License Manager, page 9

Cisco Recommendations

Cisco offers the following recommendations.

Table 3 Cisco Recommendations

If you currently use:	Do this:
Unified CM Release 6.1(1) or 6.1(1a)	Upgrade to Unified CM 6.1(1b)
A Unified CM Release 6.1(1) or 6.1(1a) Engineering Special	Contact TAC to obtain the fixes that are included in Release 6.1(1b)

Installation Note

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.

Out of Service Nodes and Cisco License Manager

Symptom

After an upgrade from Cisco Unified CallManager Release 5.1.2 to Cisco Unified Communications Manager 6.1(1), apply the 6.x software license. Restart CUCM services on all nodes. Cisco Unified Communications Manager and all services start, except Cisco License Manager. Attempts to manually restart Cisco License Manager are not successful.

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 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 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 is 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.

Clarification for Call Park Configuration

Consider the following information when you configure Call Park:

Call Park numbers cannot overlap between Cisco Unified Communications Manager servers. Ensure that each Cisco Unified Communications Manager 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, a unique call park number or range of call park extension numbers must be defined 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.

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=.

Resetting Database Replication When Reverting 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 reminding you about the requirement to reset database replication if you are reverting to an older product release. This behavior is also documented in the caveats CSCsl57629 and CSCsl57655.

utils dbreplication clusterreset

This command resets database replication on an entire cluster.

Command Syntax

utils dbreplication clusterreset

Usage Guidelines

Before you run this command, run the command **utils dbreplication stop** first on all subscribers servers, and then on the publisher server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

Command Syntax

utils dbreplication dropadmindb

Usage Guidelines

You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

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 installing RTMT. Select **Allow** to continue.

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 error 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.

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).

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 indicating that the session has timed out and redirecting you to the login window. After you log in again, you may have 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 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 error 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 error 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.

Updating the IP Address in the Server Configuration Window

Before you change the IP address of a server in the Server Configuration window in Cisco Unified Communications Manager Administration, consider the following information:

- Cisco Unified Communications Manager Administration does not prevent you from updating the IP Address field under any circumstances.
- When you attempt to change the IP address in the Server Configuration window, the following message displays after you save the configuration: “Changing the host name/IP Address of the server may cause problems with Cisco Unified Communications Manager. Are you sure that you want to continue?” Before you click OK, make sure that you understand the implications of updating this field; for example, updating this setting incorrectly may cause Cisco Unified Communications Manager to become inoperable; that is, the database may not work, you may not be able to access Cisco Unified Communications Manager Administration, and so on. In addition, updating this field without performing other related tasks may cause problems for Cisco Unified Communications Manager.
- For additional information on changing IP addresses for Cisco Unified Communications Manager, refer to the following URL:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094601.shtml

Serviceability Limitations

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.

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

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

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

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

Tip Before you perform the procedure, review the information in the " Deleting a Server" section on page 102, which provides important considerations on deleting a server.

Procedure

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

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform a 6.1(1a) installation on it by using the 6.1(1a) disk that Cisco provided in your software kit.

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

If the first node in the cluster runs 6.1(1a) and a service release (or engineering special), you must choose the **Upgrade During Install** option when the installation displays the installation options; before you choose this option, ensure that you can access the service release (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, refer to *Installing Cisco Unified Communications Manager 6.1(1).*

Step 3 After you install Cisco Unified Communications Manager, configure the subsequent node, as described in the "Configuring a Subsequent Node" section in the document, *Installing Cisco Unified Communications Manager 6.1(1).*

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*.

Cisco Unified Reporting Application

The Cisco Unified Reporting web application, which is accessed at the Cisco Unified Communications Manager console or from the Cisco Unified Communications Manager Real-Time Monitoring Tool, generates reports for troubleshooting or inspecting cluster data. You can find more information about this application in the *Cisco Unified Reporting Administration Guide*.

New and Changed Information in Cisco Unified Communications Manager 6.1(1x)

The following section describes new features and changes that are pertinent to Cisco Unified Communications Manager, Release 6.1(1x) or later. The sections may include configuration tips for the administrator, information about users, and information about where to find more information.

Basic Uninterruptible Power Supply (UPS) Integration

When Cisco Unified Communications Manager 6.0(1a) runs on an MCS 7825H2 or MCS 7835H2, basic integration to the 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 which 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.

New Service Parameters Added to Extension Mobility

Extension Mobility includes four new service parameters. You can find these new parameters at **System > Service Parameters > Cisco Extension Mobility > Advanced**.

- Validate IP Address, page 17
- Trusted List of IPs, page 18
- Allow Proxy, page 18
- Extension Mobility Cache Size, page 18

Validate IP Address

This parameter specifies whether validation of the IP address of the source that is requesting login or logout occurs.

The paramater can take values of true or false.

- If the parameter specifies true, the IP address from which an EM log in or log out request is made gets validated to ensure that it is a trusted IP address.

  Validation Procedure

  - Validation is first performed against the cache for the device to be logged in or logged out.
  - If the requesting source IP address is not found in cache, the IP address gets checked against the list of trusted IP addresses and hostnames specified in the Trusted List of IPs service parameter.
  - If the requesting source IP address is not present in the Trusted List of IPs service parameter, it is checked against the list of devices registered to Cisco Unified CallManager.

  Validation Effect

  - If the IP address of the requesting source is found in the cache or in the list of trusted IP addresses or is a registered device, the device is allowed to perform login or logout.
  - If the IP address is not found, the log in or log out attempt is blocked.
- If the parameter specifies false, the EM log in or log out request does not get validated.

Note Validation of IP addresses may increase the time required to log in or log out a device, but it offers an additional layer of security in the effort to prevent unauthorized log in or log out attempts, especially when used in conjunction with log ins from separate trusted proxy servers for remote devices.

For more information, refer to the design guidelines in the Extension Mobility documentation.

Trusted List of IPs

This parameter displays as a text box (maximum length - 1024 characters). You can enter strings of trusted IP addresses or hostnames, separated by semi-colons, in the text box. IP address ranges and regular expressions do not get supported.

Allow Proxy

Allow Proxy can take values of true or false.

- If the parameter specifies true, EM log in and log out operations using a web proxy are allowed.
- If the parameter specifies false, EM log in and log out requests coming from behind a proxy get rejected.

Note The setting you select takes effect only if the Validate IP Address parameter specifies true.

Extension Mobility Cache Size

This parameter displays as a text box in which the administrator can configure the size of the device cache maintained by Extension Mobility. The minimum value for this field is 1000 and the maximum is 20000. The default specifies 10000.

Note The value you enter takes effect only if the Validate IP Address parameter specifies true.

Disaster Recovery Manual Backup Window

Disaster Recovery System backs up CAR/CDR data automatically when you check the CCM checkbox on the Manual Backup window. The Manual Backup window no longer contains a CAR/CDR checkbox.

Cisco Unified Communications Operating System CLI Commands

This section describes Cisco Unified Communications Operating System CLI commands that are added or updated in this release.

file delete

The **file delete** command includes the parameters **dir tftp** and **license**. The **file delete** command deletes one or more files.

Command Syntax

file delete

dir tftp *directory* [**detail**]

license *filename* [**detail**]

Parameters

- **dir tftp** *directory* deletes the TFTP directory specified by *directory*. You cannot enter the wildcard character (*) in *directory*.
- **license** *filename* deletes the license file that is specified by *license*. You can enter the wildcard character (*****) as *filename* to delete all the license files.

Options

- **detail**—Displays details

Usage Guidelines

You get prompted for confirmation after entering the command.

You cannot delete directories or files that are in use.

file dump

The **file dump** command includes the new parameter **sftpdetails**. The **file dump** command dumps the contents of a file to the screen, a page at a time.

Command Syntax

file dump

sftpdetails *filename* [**hex**] [**regexp** *expression*] [**recent**]

Parameters

- **sftpdetails** specifies SFTP-related files.
- *filename* specifies the filename of the file to dump.

Options

- **hex**—Displays output in hexadecimal
- **regexp** *expression*—Displays only the lines in the file that match the regular expression *expression*.
- **recent**—Displays the most recently modified file in the directory.

Usage Guidelines

To determine which files you can dump with this command, first enter the following command:

file list sftpdetails *

The output lists the filenames that you can dump.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file fragmentation sdi

This command displays file fragmentation information about SDI log files.

Command Syntax

file fragmentation sdi

all *outfilename*

file *filename* {**verbose**}

most fragmented *number*

most recent *number*

Parameters

- **all** records information about all files in the directory in the file that is specified by *outfilename*.
- **file** displays information about the file that is specified by *filename*.
- **most fragmented** displays information about the most fragmented files.
- **most recent** displays information about the most recently logged fragmented file.
- *number* specifies the number of files to list.

Options

- **verbose**—Displays more detailed information

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file fragmentation sdl

This command displays file fragmentation information about SDL log files.

Command Syntax

file fragmentation sdl

all *outfilename*

file *filename* {**verbose**}

most fragmented *number*

most recent *number*

Parameters

- **all** records information about all files in the directory in the file that is specified by *outfilename*.
- **file** displays information about the file that is specified by *filename*.
- **most fragmented** displays information about the most fragmented files.
- **most recent** displays information about the most recently logged fragmented file.
- *number* specifies the number of files to list.

Options

- **verbose**—Displays more detailed information

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file get

The **file get** command includes the new parameters **salog**, **partBsalog**. The **file get** command sends the file to another system by using SFTP.

Command Syntax

file get

salog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

partBsalog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

Parameters

- **salog** specifies the salog log directory.
- **partBsalog** specifies the partBsalog log directory.
- *directory/filename* specifies the path to the file(s) to get. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Options

- **abstime**—Absolute time period, specified as *hh:mm:MM/DD/YY hh:mm:MM/DD/YY*
- **reltime**—Relative time period, specified as **minutes | hours | days | weeks | months** *value*
- **match**—Match a particular string in the filename, specified as *string value*
- **recurs**—Get all files, including subdirectories

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

file list

The **file list** command includes the new parameters **salog** and **partBsalog**, and **sftpdetails**. The **file list** command lists the log files in an available log directory.

Command Syntax

file list

salog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

partBsalog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

sftpdetails *filespec* [**page**] [**detail**] [**reverse**] [**date** | **size**]

Parameters

- **salog** specifies the salog log directory.
- **partBsalog** specifies the partBsalog log directory.
- **sftplog** specifies the SFTP log directory.
- *directory* specifies the path to the directory to list. You can use a wildcard character, *, for *directory* as long as it resolves to one directory.
- *filespec* specifies the file to list. Enter * to list all of the files in the directory.

Options

- **detail**—Long listing with date and time
- **date**—Sort by date
- **size**—Sort by file size
- **reverse**—Reverse sort direction
- **page**—Displays the output one screen at a time

Requirements

Command privilege level: 1 for logs, 0 for TFTP files

Allowed during upgrade: Yes

file view

The **file view** command includes a new **system-management-log** parameter. The **file view** command displays the contents of a file.

Command Syntax

file view

system-management-log

Parameters

- **system-management-log** displays the contents of the Integrated Management Logs (IML).

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

run loadxml

Run this command as a workaround when service parameters or product-specific information does not appear in the administration window as expected.

You may need to restart some services may be required after this command.

Command Syntax

run loadxml

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network dhcp

The set network dhcp command gets updated as described in this section. This command configures DHCP on Ethernet interface 0. You cannot configure Ethernet interface 1.

Command Syntax

set network dhcp eth0

enable

disable *node_ip net_mask gateway_ip*

Parameters

- **eth0** specifies Ethernet interface 0.
- **enable** enables DHCP.
- **disable** disables DHCP.
- *node_ip* is the new static IP address for the server.
- *net_mask* is the subnet mask for the server.
- *gateway_ip* is the IP address of the default gateway.

Usage Guidelines

The system asks whether you want to continue to execute this command.

Caution If you continue, this command causes the system to restart. Cisco also recommends that you restart all nodes whenever any IP address gets changed.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network restore

This command configures the specified Ethernet port to use a specified static IP address.

Caution Only use this command option if you cannot restore network connectivity by using any other **set network** commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After you run this command, you must restore your previous network configuration manually.

Caution The server temporarily loses network connectivity when you run this command.

Command Syntax

set network restore eth0 *ip-address network-mask gateway*

Parameters

- **eth0** specifies Ethernet interface 0.
- *ip-address* specifies the IP address.
- *network-mask* specifies the subnet mask.
- *gateway* specifies the IP address of the default gateway.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show ctl

This command displays the contents of the Certificate Trust List (CTL) file on the server. It notifies you if the CTL is not valid.

Command Syntax

show ctl

show diskusage

This command displays information about disk usage on the server.

Command Syntax

show diskusage

activelog {**filename** *filename* | **directory** | **sort**}

common {**filename** *filename* | **directory** | **sort**}

inactivelog {**filename** *filename* | **directory** | **sort**}

install {**filename** *filename* | **directory** | **sort**}

tftp {**filename** *filename* | **directory** | **sort**}

tmp {**filename** *filename* | **directory** | **sort**}

Parameters

- **activelog** displays disk usage information about the activelog directory.
- **common** displays disk usage information about the common directory.
- **inactivelog** displays disk usage information about the inactivelog directory.
- **install** displays disk usage information about the install directory.
- **tftp** displays disk usage information about the TFTP directory.

- **tmp** displays disk usage information about the TMP directory.

Options

- **filename** *filename*—Saves the output to a file that is specified by *filename*. The **platform/cli** directory stores these files. To view saved files, use the **file view activelog** command.
- **directory**—Displays just the directory sizes.
- **sort**—Sorts the output based on file size. file sizes display in 1024-byte blocks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show environment

This command displays information about the server hardware.

Command Syntax

show environment

fans

power-supply

temperatures

Parameters

- **fans** displays information that was gathered by fan probes
- **power-supply** displays information that was gathered by power supply probes
- **temperatures** displays information that was gathered by temperature probes

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show iptables

Be aware that the **show iptables** command was removed. The **utils firewall list** command now displays similar information.

show process

This command displays information about process that is running on the system.

Syntax

show process

list [**file** *filename*] [**detail**]

load [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu | memory| time**] [**page**]

name *process* [**file** *filename*]

open-fd *process-id* [**,** *process-id2*]

search *regexp* [**file** *filename*]

using-most cpu [*number*] [**file** *filename*]

using-most memory [*number*] [**file** *filename*]

Parameters

- **list** displays a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes.
- **load** displays the current load on the system.
- **name** displays the details of processes that share the same name and indicates their parent-child relationship.
- **open-fd** lists the open file descriptors for a comma-separated list of process IDs.
- **search** searches for the pattern that is specified by the regular expression *regexp* in the output of the operating system-specific process listing.
- **using-most cpu** displays a list of the most CPU-intensive processes.
- **using-most memory** displays a list of the most memory-intensive processes.

Options

- **file** *filename*—outputs the results to the file that is specified by *filename.*
- **detail**—displays detailed output.
- **cont**—repeats the command continuously.
- **clear**—clears the screen before displaying output.
- **noidle**—ignore the idle/zombie processes.
- **num** *number*—displays the number of processes that are specified by *number.* The default number of processes equals 10. Set *number* to **all** to display all processes.
- **thread**—displays threads.
- [**cpu | memory | time**]—sorts output by CPU usage, memory usage, or time usage. The default specifies to sort by CPU usage.
- **page**—displays the output in pages.
- *process*—specifies the name of a process.
- *process-id*—specifies the process ID number of a process.
- *regexp*—indicates a regular expression.
- *number*—specifies the number of processes to display. The default equals 5.

show tech database

This command includes the new parameters **dump** and **session**.

Command Syntax

show tech database

dump

sessions

Parameters

- **dump** creates a CSV file of the entire database.
- **sessions** redirects the session and SQL information of the present session IDs to a file.

show tech network

The show tech network command gets updated as described in this section. This command displays information about the network aspects of the server.

Command Syntax

show tech network

all [**page**] [**search** *text*] [**file** *filename*]

hosts [**page**] [**search** *text*] [**file** *filename*]

interfaces [**page**] [**search** *text*] [**file** *filename*]

resolv [**page**] [**search** *text*] [**file** *filename*]

routes [**page**] [**search** *text*] [**file** *filename*]

sockets {**numeric**}

Parameters

- **all** displays all network tech information.
- **hosts** displays information about hosts configuration.
- **interfaces** displays information about the network interfaces.
- **resolv** displays information about hostname resolution.
- **routes** displays information about network routes.
- **sockets** displays the list of open sockets.

Options

- **page**—displays one page at a time.
- **search** *text*—searches the output for the string that is specified by *text*. Be aware that the search is case insensitive.
- **file** *filename*—outputs the information to a file.
- **numeric**—displays the numerical addresses of the ports instead of determining symbolic hosts. Consider it as equivalent to running the Linux shell command netstat [-n] command.

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech runtime

The show tech runtime command gets updated as described in this section. This command displays runtime aspects of the server.

Command Syntax

show tech runtime

all [**page**] [**file** *filename*]

cpu [**page**] [**file** *filename*]

disk [**page**] [**file** *filename*]

env [**page**] [**file** *filename*]

memory [**page**] [**file** *filename*]

Parameters

- **all** displays all runtime information.
- **cpu** displays CPU usage information at the time that the command is run.
- **disk** displays system disk usage information.
- **env** displays environment variables.
- **memory** displays memory usage information.

Options

- **page**—displays one page at a time
- **file** *filename*—outputs the information to a file

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech system

The show tech system command gets updated as described in this section. This command displays system aspects of the server.

Command Syntax

show tech system

all [**page**] [**file** *filename*]

bus [**page**] [**file** *filename*]

hardware [**page**] [**file** *filename*]

host [**page**] [**file** *filename*]

kernel [**page**] [**file** *filename*]

software [**page**] [**file** *filename*]

tools [**page**] [**file** *filename*]

Parameters

- **all** displays all of the system information.
- **bus** displays information about the data buses on the server.
- **hardware** displays information about the server hardware.
- **host** displays information about the server.
- **kernel modules** lists the installed kernel modules.
- **software** displays information about the installed software versions.
- **tools** displays information about the software tools on the server.

Options

- **page**—displays one page at a time.
- **file** *filename*—outputs the information to a file.

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils create report

This command creates reports about the server in the platform/log directory.

Command Syntax

utils create report

hardware

platform

Parameters

- **hardware** creates a system report that contains disk array, remote console, diagnostic, and environmental data.
- **platform** collects the platform configuration files into a TAR file.

Usage Guidelines

You are prompted to continue after you enter the command.

After creating a report, use the command **file get activelog platform/log/***filename*, where *filename* specifies the report filename that displays after the command completes, to get the report.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication clusterreset

This command resets database replication on an entire cluster.

Command Syntax

utils dbreplication clusterreset

Usage Guidelines

Before you run this command, run the command **utils dbreplication stop** first on all subscribers servers, and then on the publisher server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

Command Syntax

utils dbreplication dropadmindb

Usage Guidelines

You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication setrepltimeout

You can use this command to set the timeout for database replication on large clusters.

Command Syntax

utils dbreplication setrepltimeout *timeout*

Options

- *timeout*—provides the new database replication timeout, in seconds. Ensure the value is between 300 and 3600.

Usage Guidelines

The default database replication timeout equals 5 minutes. All subscriber servers that are requesting replication within 5 minutes get on the broadcast list and get replicated. For large clusters, you can use the command to increase the default timeout.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils diagnose

This command enables you to diagnose and attempt to automatically fix system problems.

Command Syntax

utils diagnose

fix

list

module *module_name*

test

version

Parameters

- **fix** runs all diagnostic commands and attempts to fix problems.
- **list** lists all available diagnostic commands.
- **module** runs a single diagnostic command or group of commands and attempts to fix problems.
- **test** runs all diagnostic commands but does not attempt to fix problems.
- **version** displays the diagnostic framework version.
- *module_name* specifies the name of a diagnostics module.

utils firewall

This command manages the firewall on the node.

Command Syntax

utils firewall

disable {*time*}

enable

list

status

Parameters

- **disable** disables the firewall.
- *time* specifies the duration for which the firewall is disabled, in one of these formats:
  - [0-1440]**m** to specify a duration in minutes.
  - [0-24]**h** to specify a duration in hours.
  - [0-23]**h**[0-60]**m** to specify a duration in hours and minutes.

  If you do not specify a time, the default equals 5 minutes.

- **enable** enables the firewall.
- **list** displays the current firewall configuration.
- **status** displays the status of the firewall.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network connectivity

This command verifies the node network connection to the first node in the cluster. Be aware that it is only valid on a subsequent node.

Command Syntax

utils network connectivity

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils snmp

The **utils snmp** command includes the new parameters **get**, **hardware-agents**, and **walk**.

Command Syntax

utils snmp

get *version community ip-address object* [*file*]

hardware-agents [**status** | **restart**]

walk *version community ip-address object* [*file*]

Parameters

- **get** displays the value of the specified SNMP object.
- **hardware-agents status** displays the status of the hardware agents on the server.
- **hardware-agents restart** restarts the hardware agents on the server.
- **walk** walks the SNMP MIB, starting with the specified SNMP object.
- *version* specifies the SNMP version. Possible values include 1 or 2c.
- *community* specifies the SNMP community string.
- *ip-address* specifies the IP address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IP address of another node in the cluster to run the command on that node.
- *object* specifies the SNMP Object ID (OID) to get.
- *file* specifies a file in which to save the command output.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils system switch-version

For this modified commandthe **switch-version** parameter includes the new option **nodatasync**. The **utils system switch-version** command allows you to restart the system on the inactive partition.

Command Syntax

utils system

switch-version [**nodatasync**]

Options

- **nodatasync**—Switches product versions without synchronizing User Facing Feature Data (UFF data) between the active and inactive partitions.

Usage Guidelines

A warning message displays, and you are prompted for confirmation before this command runs with the **nodatasync** option.

If you use the **nodatasync** option, any changes to UFF data on the active partition will be lost. You should use this option only to force the versions to switch if the system otherwise will not switch versions because a data synchronization failure occurred. For more information about UFF data, refer to the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a008085f619.html#wp1043639

Note Administrative changes that are made on the active partition, such as adding new phones, are not synchronized when you switch versions. UFF data gets synchronized when you switch versions, unless you use the **nodatasync** option.

This option does not support command auto-completion. You must enter the entire option name.

Installation, Upgrade, Migration, and Disaster Recovery

The following sections describe the changes that were made to the installation, upgrade, and disaster recovery procedures in Cisco Unified Communications Manager 6.1(1a):

- Installation Overview, page 33
- Where to Find More Information, page 34

Installation Overview

For 6.1(1a), the Cisco Unified Communications Manager installation process includes the following new features:

- Allows you to set the maximum transmission unit (MTU) size
- Validates that a subsequent node can communicate with the first node

MTU Size Parameter

During installation, you can configure the MTU size parameter. The MTU size represents the largest packet, in bytes, that the host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, 1500 bytes.

Note You can also set the MTU size after installation by using the CLI command, **set network mtu**.

Connectivity Validation

To ensure successful installation of a subsequent node, the system now validates that the subsequent node can connect with the first node.

If connectivity validation fails, the installation process stops, and the system prompts you to reenter the network configuration information. After you update the network configuration information, you can continue with the installation.

When connectivity validation succeeds, you can choose whether you want the installation process to continue uninterrupted or stop and display a successful validation message. To display the confirmation message, check the check box for **Show confirmation on successful connection to first node** on the First Node Access Configuration window.

Enhanced Documentation

For Release 6.1, installation and upgrade documentation enhancements to cover additional pre- and post-installation tasks, as well as specific steps for adding a new subscriber node to an existing cluster.

The Release 6.1 documentation set also includes a new document that describes the procedures for replacing a cluster or a single server in an existing cluster, *Replacing a Cluster or Single Server for Cisco Unified Communications Manager Release 5.1(3)*.

Changing IP Addresses

The document *Changing the IP Address for Cisco Unified Communications Manager 5.x and 6.x Servers* describes how to change the IP address of Cisco Unified Communications Manager servers for releases 5.x and 6.x.

Where to Find More Information

- *Disaster Recovery System Administration Guide*
- *Data Migration Assistant User Guide*
- *Upgrading Cisco Unified Communications Manager Release 6.1(1)*
- *Installing Cisco Unified Communications Manager Release 6.1(1)*
- *Replacing a Cluster or Single Server for Cisco Unified Communications Manager 6.1(1)*

Cisco Unified Communications Operating System Administration

For Cisco Unified Communications Manager 6.1(1a), you can perform many common system administration functions through the Cisco Unified Communications Operating System.

This chapter comprises the following topics:

- Where to Find More Information, page 34

Overview

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

Browser Requirements

You can access Cisco Unified Communications Manager Administration by using the following browsers:

- Microsoft Internet Explorer version 6 and Internet Explorer 7
- Netscape Navigator version 7.1

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

Where to Find More Information

- *Cisco Unified Communications Operating System Administration Guide*

Cisco Unified Communications Manager Administration

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

- Browser Requirements for Cisco Unified Communications Manager Administration, page 35
- Service Parameter and Enterprise Parameter Changes, page 36
- Menu Changes, page 37
- Where to Find More Information, page 38

Browser Requirements for Cisco Unified Communications Manager Administration

The following browser requirements apply to Cisco Unified Communications Manager Administration:

- Netscape 7.1
- Microsoft Internet Explorer (IE) 6 and 7

Tip Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration website as untrusted and provides a certificate error, even when the trust store contains the server certificate. Refer to the *Cisco Unified Communications Manager Security Guide* for the certificate download procedure.

Service Parameter and Enterprise Parameter Changes

Cisco Unified Communications Manager 6.1 supports the following service parameter changes:

- SIP TCP Unused Connection Timer (service parameter introduced in 5.1(3))—This parameter, which supports the Cisco CallManager service, specifies the time, that is, the interval, in which Cisco Unified Communications Manager determines whether the TCP connection is still in use. When the timer expires, Cisco Unified Communications Manager checks for traffic in the preceding block of time, as specified by the value that you configure for the parameter; for example, 20 minutes. If no traffic occurred during that time, Cisco Unified Communications Manager closes the TCP connection. If traffic occurred, the TCP connection remains open until the timer expires again, at which point Cisco Unified Communications Manager checks for traffic again.

  For example, if the value for the parameter equals 20 minutes and the timer expires at 3:00, Cisco Unified Communications Manager examines the time from 2:40 to 3:00. If traffic occurred during that time, the connection remains open until the next examination at 3:20. If no traffic occurred from 3:00 to 3:20, Cisco Unified Communications Manager closes the TCP connection at or shortly after 3:20. If traffic occurred from 3:00 to 3:20, the TCP connection remains open until Cisco Unified Communications Manager checks for traffic again at 3:40, and so on.

  After you update this parameter, you must restart the Cisco CallManager service for the changes to take effect.

  For the default, maximum, and minimum values for the parameter, access the parameter in Cisco Unified Communications Manager Administration and either click the name of the service parameter or click the ? button in the Service Parameter Configuration window.

Note If you have other devices in the path of a call flow that include a SIP timeout, like a firewall, adjust those timeouts to be slightly longer than two times the value of this parameter.

- Join Across Lines Policy—This parameter, which supports the Cisco CallManager service, enables the enhanced join feature in Cisco Unified Communications Manager. The enhanced join feature allows a phone user to press the Join softkey and then the line button of an existing call to convert an existing call to an Ad Hoc conference. The user who pressed the Join softkey becomes the conference initiator and can add more participants to the conference or utilize conference chaining, and other Ad Hoc conference features as desired. Valid values specify On (enable the enhanced join functionality) or Off (disable the enhanced join functionality). The default setting for this required field specifies Off.
- Single Button Barge/CBarge Policy—This parameter, which supports the Cisco CallManager service, determines whether phone users have single-button access for barge and conference barge (cBarge). When enabled, single-button capability allows users to barge/cBarge into an existing shared line call simply by pressing the line button that is associated with the call that they want to barge/cBarge into. Valid values specify Off (single-button access is not available; use the Barge and cBarge softkeys instead), Barge (when the user presses the line key, he or she will join the call via barge), or CBarge (when the user presses the line key, he or she will join the call via cBarge). The default setting for this required field specifies Off.

Tip For the change to take effect in a cluster, you must either restart the Cisco CallManager service, reset all affected device pools, or restart/reset all affected phones.

- Auto select DN on any Partition (enterprise parameter introduced in 5.1(3))—This parameter specifies whether the Directory Number Configuration window automatically selects the first matching DN to populate the window. The default specifies False, which means that the DN/Partition name gets used to populate the DN window. If the parameter is set to True and the DN is changed, the first entry that matches the DN gets used to populate the window.
- Report Socket Connection Timeout and Report Socket Read Timeout (enterprise parameter introduced in 5.1.(3))—These two parameters support the Cisco Unified Reporting application, as follows: The Report Socket Connect Timeout parameter specifies the maximum number of seconds that the application uses when attempting to connect to another server. Increase this time if you experience connection issues on a slow network. The range for this required field specifies 5 to 120 seconds, and the default value specifies 10 seconds.

  The Report Socket Read Timeout parameter specifies the maximum number of seconds that the application uses when reading data from another server. Increase this time if you experience connection issues on a slow network. For this required field, the range goes from 5 to 600 seconds, and the default value specifies 60 seconds.
- Inbound Calling Search Space for Remote Destination --This parameter specifies the calling search space (CSS) that Cisco Unified Communications Manager (Unified CM) utilizes to route an incoming call from a configured Remote Destination. Valid values specify Trunk or Gateway Inbound Calling Search Space (Unified CM uses the inbound calling search space of the trunk or gateway from which the call arrived) or Remote Destination Profile + Line Calling Search Space (Unified CM uses the concatenation of the calling search spaces on the line and Remote Destination profile that is associated with the remote destination that was matched). This parameter does not affect calls that do not match a Remote Destination because they always use the trunk or gateway inbound CSS. For calls that come from a Remote Destination (the calling party number matches the Remote Destination number), choose Remote Destination Profile + Line Calling Search Spaces to use those calling search spaces to route the call instead of using the Trunk/Gateway Calling Search Space. The digits that come from the trunk or gateway must be formatted in a way that can be dialed by using the Remote Destination Profile + Line Calling Search Spaces.

  After you update this parameter, you must restart the Cisco CallManager service for the changes to take effect.

  For the default, maximum, and minimum values for the parameter, access the parameter in Cisco Unified Communications Manager Administration and either click the name of the service parameter or click the ? button in the Service Parameter Configuration window.

Menu Changes

The following changes occurred in the Cisco Unified Communications Manager Administration menus:

- **System > Device Pool**—Single Button Barge/cBarge and Join Across Lines (new fields)
- **System > Service Parameters > Service Parameter**—New service parameters (See the " Service Parameter and Enterprise Parameter Changes" section on page 36.)
- **System > Licensing > License Unit Calculator**—Mobility Enabled End User (Adjunct) (new row)
- **Call Routing > Intercom > Intercom Directory Number**—Default Activated Device (new setting)
- **Device > Phone**—Single Button Barge/cBarge and Join Across Lines (new fields)
- **Device > Device Settings > Default Device Profile**—Single Button Barge/cBarge and Join Across Lines (new fields)
- **Device > Device Settings > Device Profile**—Single Button Barge/cBarge and Join Across Lines (new fields)

- **Device > Device Settings > SIP Profile**—Reroute Incoming Request to new Trunk based on (new field)
- **User Management > End User**—Primary User Device (new field); works in conjunction with Enable Mobility check box (changed functionality)
- **Bulk Administration > Users > Update User**s—Primary User Device (new field); works in conjunction with Enable Mobility check box.
- **Bulk Adminstration > User Device Profile > Add/Update Intercom DNs**—New submenu to add and update intercom DNs to User Device Profiles in bulk.
- **Bulk Administration > User Device Profiles > UDP Template**—Single Button Barge/cBarge and Join Across Lines (new fields).
- **Bulk Adminstration > User Device Profiles > Add/Update Intercom DNs**—New submenu to add and update intercom DNs to User Device Profiles in bulk.

Where to Find More Information

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

Cisco Unified Communications Manager Features and Applications

The following sections describe the Cisco Unified Communications Manager 6.1 feature and application enhancements:

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.

Intercom for Cisco Extension Mobility

Cisco Unified Communications Manager Administration Configuration Tips

Beginning with Release 6.1(1a) of Cisco Unified Communications Manager, intercom directory numbers require configuration of the Default Activated Device field in the Intercom Directory Number Configuration window if the intercom directory number is to be active.

Beginning with Release 6.1(1a) of Cisco Unified Communications Manager, you can also configure intercom directory numbers for use with Cisco Extension Mobility by configuring the Default Activated Device field.

Cisco Extension Mobility uses a default device that is configured for an intercom line. An intercom line only gets presented on the default device. You can assign an intercom line to a device profile.

The system presents an intercom line to a user who uses Cisco Extension Mobility to log in to a phone that supports the intercom feature if the device profile that the user uses to log in has an intercom line that is provisioned. The phone must act as the default device for that intercom line. When a user logs on to a device that is not the default device, the intercom line does not get presented.

GUI Change

Call Routing > Intercom > Intercom Directory Number—Displays a new row for Default Activated Device. For the intercom feature to function for users who log in to phones remotely by using Cisco Extension Mobility ensure that the new Default Activated Device is configured.

Service Parameter and Enterprise Parameter Changes

No service parameter or enterprise parameter considerations exist for configuration of the intercom feature with Cisco Extension Mobility.

Installation/Upgrade (Migration) Considerations

For an existing intercom line that is assigned to a device, migration from release 6.0(1) of Cisco Unified Communications Manager to release 6.1(1a) or later automatically designates the intercom default device for that intercom line.

Serviceabilty Considerations

No serviceability considerations exist for configuration of the intercom feature with Cisco Extension Mobility.

BAT Considerations

For information on how the intercom feature works with Cisco Extension Mobility in the Bulk Administration Tool, see the " Cisco Unified Communications Manager Bulk Administration Tool" section on page 47.

CAR/CDR Considerations

No CAR/CDR considerations exist for configuration of the intercom feature with Cisco Extension Mobility.

Security Considerations

No security considerations exist for configuration of the intercom feature with Cisco Extension Mobility.

CTI Considerations

No administrator-configuratble CTI considerations exist for configuration of the intercom feature with Cisco Extension Mobility.

User Tips

For information on how the intercom feature works with Cisco Extension Mobility on Cisco Unified IP Phones, see the discussion of Intercom with Cisco Extension Mobility in the " Cisco Unified IP Phones" section on page 52.

For More Information

- Intercom Directory Number Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Device Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Cisco Extension Mobility chapter, *Cisco Unified Communications Manager Features and Services Guide*
- Intercom chapter, *Cisco Unified Communications Manager Features and Services Guide*

Join Across Lines

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

- **System > Service Parameters > Service Parameter Configuration**— When you configure the service parameters, a policy setting exists for Join Across Lines. Set the Join Across Lines feature t to Off or On. The default setting specifies **Off**.
- **System > Device Pool**— When you configure a new device pool, a new row for Join Across Lines. exists. You can set the Join Across Lines feature to Off, On, or Default. If it is set to Default, the devices in this device pool will use the service parameter setting for the Join Across Lines feature.
- **Device > Device Settings > Default Device Profile**—When you add a new default device profile configuration for a SCCP phone, a new row for Join Across Lines exists. You can set the Join Across Lines featureto 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.
- **Device > Device Settings > Device Profile**—When you add a new device profile configuration for a SCCP phone, 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.

- **Device > Phone**—When you add a new phone configuration for a SCCP phone, a new row for Join Across Lines exists. 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.

BAT Considerations

For information on how you can configure join across lines in BAT, see the " Cisco Unified Communications Manager Bulk Administration Tool" section on page 47.

AXL and CTI Considerations

For information on join across lines works with AXL, see the " Cisco and Third-Party APIs" section on page 57.

User Tips

For information phone support for join across lines, see the " Cisco Unified IP Phones" section on page 52.

For More Information

- Understanding Directory Numbers chapter, *Cisco Unified Communications Manager System Guide*
- Cisco IP Phone Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Default Device Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Device Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*

Licensing for Cisco Unified Mobility

This section contains information on licensing for Cisco Unified Mobility.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

- System > Licensing > License Unit Calculator—Displays a row for Mobility Enabled End User (Adjunct), which displays the number of device license units that are consumed and credited for adjunct devices that are used specifically for Cisco Unified Mobility.
- User Management > End User—Displays the Enable Mobility check box, which triggers device license units to get consumed; works in conjunction with the Primary User Device drop-down list box.

  If you check the Enable Mobility check box and fail to choose an adjunct device from the Primary User Device drop-down list box, four device license units (DLUs) get consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.

  If you enable Cisco Unified Mobility and later choose an adjunct device from the Primary User Device drop-down list box, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.
- User Management > End User—Displays the Primary User Device drop-down list box, which controls the number of device license units that are consumed for adjunct devices for Mobile Connect; works in conjunction with the Enable Mobility check box in the End User Configuration window.

After you check the Enable Mobility check box, choose an adjunct device that you want to assign to the user specifically for Cisco Unified Mobility. For example, choose a device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility.

Before you choose an adjunct device, consider the following information:

- Only devices that consume two or more device license units (DLUs) display in the drop-down list box.
- For Cisco Unified Mobility, you cannot assign the same device to multiple users, so only the devices that you can assign display in the drop-down list box.
- If you check the Enable Mobility check box and choose a device from the drop-down list box, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the Licensing Unit Calculation window.
- If you delete the device from Cisco Unified Communications Manager Administration or remove the assignment after you enable Mobile Connect, two DLUs get consumed after you delete the device or remove the assignment, as indicated in the Mobility Enabled End Users row in the License Unit Calculation window.

BAT Considerations

For information on how Cisco Unified Mobility and licensing work for Bulk Administration Tool, see the " Cisco Unified Communications Manager Bulk Administration Tool" section on page 47.

AXL and CTI Considerations

For information on how Cisco Unified Mobility and licensing work for AXL, see the " Cisco and Third-Party APIs" section on page 57.

For More Information

- Licensing chapter, *Cisco Unified Communications Manager System Guide*
- End User Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Mobile Connect and Mobile Voice Access chapter, *Cisco Unified Communications Manager Features and Services Guide* (primarily about Cisco Unified Mobility, not licensing)

Single Button Barge

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

- **System > Service Parameters > Service Parameter Configuration**— When you configure the service parameters, a new policy setting for Single Button Barge/cBarge exists. You can set the Single Button Barge/cBarge feature to Off, Barge, or cBarge. The default setting specifies **Off**.
- **System > Device Pool**— When you configure a new device pool, a new row for Single Button Barge/cBarge exists. You can set the Single Button Barge/cBarge feature to Off, Barge, cBarge, or Default. If it is set to Default, the devices in this device pool will use the service parameter setting for the Join Across Lines feature.
- **Device > Device Settings > Default Device Profile**—When you add a new default device profile configuration for a SCCP phone, a new row for Single Button Barge/cBarge exists. 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.

- **Device > Device Settings > Device Profile**—When you add a new device profile configuration for a SCCP phone, a new row for Single Button Barge/cBarge exists. You can set the Single Button Barge/cBarge feature can be set 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.
- **Device > Phone**—When you add a new phone configuration for a SCCP phone, a new row for Single Button Barge/cBarge exists. 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.

BAT Considerations

For information on how you can configure single button barge in BAT, see the " Cisco Unified Communications Manager Bulk Administration Tool" section on page 47.

AXL and CTI Considerations

For information on how join across lines works with AXL, see the " Cisco and Third-Party APIs" section on page 57.

User Tips

For information on phone support for single button barge, see the " Cisco Unified IP Phones" section on page 52.

For More Information

- Barge and Privacy chapter, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco IP Phone Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Default Device Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Device Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phones chapter, *Cisco Unified Communications Manager System Guide*

SIP Trunk Identification

This section contains information on how Cisco Unified Communications Manager identifies the SIP trunk to use for a call.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

- Device > Device Settings > SIP Profile—Displays the Reroute Incoming Request to new Trunk based on drop-down list box; the SIP trunk that you configure inherits the configuration from the SIP profile that you apply to the trunk.

  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 the Reroute Incoming Request to new Trunk based 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.

AXL and CTI Considerations

For information on SIP trunk identification and AXL, see the " Cisco and Third-Party APIs" section on page 57.

For More Information

- Understanding Session Internet Protocol chapter, *Cisco Unified Communications Manager System Guide*
- SIP Profile Configuration chapter, *Cisco Unified Communications Manager Administration Guide*

Thai Language Support

Cisco Unified Communications Manager Release 6.1 supports Thai locales on Cisco Unified Communications Manager user interfaces and Thai text on phone screen displays for the following Cisco Unified IP phones.

Supported Cisco Unified IP Phones (SCCP and SIP)

7975G, 7971G-GE, 7970G, 7965G, 7962G, 7961G-GE, 7961G, 7945G, 7942G, 7941G-GE, 7941G, 7931G (SCCP only)

Turkish Language Support

Cisco Unified Communications Manager Release 6.1 supports Turkish locales on Cisco Unified Communications Manager user interfaces and Turkish text on phone screen displays for the following Cisco Unified IP phones.

Supported Cisco Unified IP Phones (SCCP and SIP)

7975G, 7971G-GE, 7970G, 7965G, 7962G, 7961G-GE, 7961G, 7945G, 7942G, 7941G-GE, 7941G, 7931G (SCCP only)

Phone Button Template, Line, and Security Enhancements for the Nokia S60 Device

In Cisco Unified Communications Manager 6.1, the following enhancements exist for the Nokia S60, the dual-mode device that you can use with Cisco Unified Mobility.

Cisco Unified CallManager Administration Configuration Tips and GUI Changes

You can configure a phone security profile for the Nokia S60 in the Phone Security Profile Configuration window in Cisco Unified Communications Manager Administration 6.1 (**System > Security Profile > Phone Security Profile**). From the Device Security Mode drop-down list box, you can choose Nonsecure, Authenticated, or Encrypted, as described in the *Cisco Unified Communications Manager Security Guide*.

In the Phone Configuration window (**Device > Phone**), you can configure a phone button template for the Nokia S60 by choosing the Nokia S60 phone template from the Phone Button Template drop-down list box.

In the Association Information pane in the Phone Configuration window for the Nokia S60, you can configure up to two lines and assign them to the device, as described in the *Cisco Unified Communications Manager Administration Guide*. You can configure additional lines under the Unassigned Associated Items pane.

In the Find and List Phone Button Template window (**Device > Device Settings > Phone Button Template**), you can view and copy the Standard Nokia S60 SCCP phone button template.

Installation/Upgrade (Migration) Considerations

Consider installing the latest 6.1(1a) compatible Nokia .cop file as optional; that is, you can use the pre-6.1(1a) mobility configuration, such as Remote Destination Profiles and Remote Destinations, for the Nokia S60 devices without installing the latest 6.1(1a) compatible Nokia .cop file. Before you can use the 6.1(1a) enhancements for the Nokia S60 in Cisco Unified Communications Manager 6.1, however, you must install the latest 6.1(1a) compatible Nokia .cop file.

If you configured Nokia S60 devices by using the pre-6.1(1a) Nokia .cop file, install the latest 6.1(1a) compatible Nokia S60 .cop file before you upgrade to Cisco Unified Communications Manager 6.1. If you choose not to upgrade to Cisco Unified Communications Manager 6.1(1a) after you install the latest Nokia S60 .cop file, your existing Nokia S60 devices do not automatically migrate as dual-mode phones that are supported with Cisco Unified Mobility after you upgrade to Cisco Unified Communications Manager 6.1(1a). For additional migration considerations, see the following scenarios:

- Scenario 1—You installed a pre-6.1(1a) Nokia .cop file, provisioned Nokia S60 devices in a pre-6.1(1a) Cisco Unified Communications Manager release, and now want to upgrade to Cisco Unified Communications Manager 6.1(1a)

  If you installed the pre-6.1(1a) Nokia .cop file, configured single-mode remote destinations for mobile destination numbers in a previous Cisco Unified Communications Manager release, and now want to use the features (for example, Mobility Identity) that the latest 6.1(1a) compatible Nokia .cop file supports, install the latest 6.1(1a) compatible Nokia .cop file before you perform the Cisco Unified Communications Manager 6.1 upgrade. After you perform the upgrade to 6.1(1a), manually delete the remote destinations in Cisco Unified Communications Manager Administration and reconfigure the destination numbers as dual-mode Mobility Identity.

- Scenario 2—This scenario applies if you upgraded to Cisco Unified Communications Manager 6.1(1a) before you installed the latest 6.1(1a) compatible Nokia .cop file.

In this situation, existing Nokia S60 devices do not automatically migrate after you install the latest 6.1(1a) compatible Nokia .cop file. To work around this limitation, you must manually delete all existing Nokia S60 devices from Cisco Unified Communications Manager Administration (or BAT) 6.1(1a) and reconfigure the devices after you install the latest 6.1(1a) compatible Nokia .cop file. Remember to reset the devices after you configure them.

For additional Nokia S60 configuration considerations, see the " Problem Configuring Mobility Identity for Nokia S60 Device in Cisco Unified Communications Manager Administration" section on page 13

BAT Considerations

You can use BAT to configure the Nokia S60 device.

Security Considerations

You can configure a phone security profile for the Nokia S60 in the Phone Security Profile Configuration window in Cisco Unified Communications Manager Administration 6.1 (**System > Security Profile > Phone Security Profile**). From the Device Security Mode drop-down list box, you can choose Nonsecure, Authenticated, or Encrypted, as described in the *Cisco Unified Communications Manager Security Guide*.

For More Information

- *Cisco Unified Communications Manager Administration Guide* (info on Cisco Unified Mobility, phone configuration, and phone button templates, not specifically on the Nokia S60 device)
- *Cisco Unified Communications Manager Features and Services Guide* (info on Cisco Unified Mobility, not the Nokia S60 device)
- *Cisco Unified Communications Manager System Guide* (info on Cisco Unified Mobility, phones, and phone button templates, not specifically on the Nokia S60 device)
- *Cisco Unified Communications Manager Security Guide* (does not provide information on the Nokia S60 device)

Cisco Unified Communications Manager Bulk Administration Tool

The following sections contain information regarding changes and additions that have been made to the Cisco Unified Communications Manager Bulk Administration Tool.

GUI Changes

The following GUI changes exist in this release of BAT:

- Single Button Barge (new field)—This represents a new field in the Phone Template Configuration window and when you add a new phone configuration for a SCCP phone, a new row for Single Button Barge/cBarge exists. 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. You can access this window through **Phones > Phone Template**.
- Join Across Lines (new field)—This represents a new field in the Phone Template Configuration window and when you add a new phone configuration for a SCCP phone, a new row for Join Across Lines exists. 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. You can access this window through **Phones > Phone Template**.

- Single Button Barge (new field)—This represents a new field in the UDP Template configuration window, and when you add a new device profile configuration for a SCCP phone, a new row for Single Button Barge/cBarge exists. 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. You can access this window through **User Device Profiles > UDP Template**.
- Join Across Lines (new field)—This represents a new field in the UDP Template configuration window, and when you add a new device profile configuration for a SCCP phone, a new row for Join Across Lines exists. 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. You can access this window through **User Device Profiles > UDP Template**.
- Add/Update Intercom DNs—This represents a new submenu in the User Device Profile menu in BAT. You can use the Add/Update Intercom utility in the User Device Profile menu to add or update intercom DNs in bulk to Cisco Unified Communications Manager server. To access this feature choose **Bulk Administration > User Device Profiles> Add/Update Intercom DNs**.
- Primary User Device (new field)—This new field in the Mobility Information section of the End User Configuration page controls the number of device license units that are consumed for adjunct devices for Mobile Connect.It works in conjunction with the Enable Mobility check box in the End User Configuration window. You can access this window through **Users > Update Users**.

Cisco Unified Serviceability

This section contains these subsections:

Collecting Installation Logs

Trace and Log Central now allows the collection of installation logs. In the Cisco Unified Communications Manager Real-Time Monitoring Tool Trace and Log Central window, double-click **Collect Install Logs**. The Collect Install Logs wizard launches and steps you through the rest of the process.

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

Database Summary Includes Database Replication Information

RTMT displays information on predefined Cisco Unified Communications Manager objects in the monitoring pane when you select Communications Manager in the quick launch channel. It monitors the predefined objects on all nodes in the cluster. The Service category includes the Database Summary that now provides the number of replicates that have been created and the status of the replication in addition to the other types of connection information that was previously provided.

To display information on the database, choose **CallManager > Service > Database Summary**.

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

New Preconfigured Alerts in Cisco Unified Serviceability

The following list shows preconfigured alerts that are now available:

- ServerDown: This alert gets triggered whenever the active AMC is unable to talk to a remote host.
- HardwareFailure: This alert gets triggered whenever a corresponding HardwareFailure alarm/event occurs.
- SDLLinkOutOfService: This alert gets triggered whenever a corresponding SDLLinkOOS alarm/event occurs.
- DBReplicationFailure: This alert gets triggered whenever the corresponding perfmon counter “replication status” has values other than zero (init) and two (success).
- SystemVersionMismatched: This alert gets triggered whenever a mismatch exists in system version.

RTMT Critical Services

Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT) provides new states for the critical services that display in RTMT. The Critical Services monitoring category (choose **Monitor > Server > Critical Services** or click the **Server** button and **Critical Services** icon) provides the name of the critical service, the status (whether the service is starting, up, stopping, down, stopped by the administrator, not activated, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the Cisco Unified Communications Manager server. For a specific description of each state, review the following information:

- starting (new state)—This state indicates that the service is currently starting, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability.
- up—This state indicates that the service is currently running, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability.
- stopping (new state)—This state indicates that the service is currently stopping, as indicated in the Critical Services pane and in Control Center in Cisco Unified Serviceability.
- down—This state indicates that the service stopped running unexpectedly; that is, you did not perform a task that stopped the service. The Critical Services pane indicates that the service is down.

Tip The CriticalServiceDown alert gets generated when the service status equals down (not for other states).

- stopped by Admin (new state)—This state indicates that you performed a task that intentionally stopped the service; for example, the service stopped because you backed up or restored Cisco Unified Communications Manager, performed an upgrade, stopped the service in Cisco Unified Serviceability or the Command Line Interface (CLI), and so on. The Critical Services pane indicates the status.
- not activated—This state indicates that the service is not currently activated, as indicated in the Critical Services pane and in Service Activation in Cisco Unified Serviceability.
- unknown state—This state indicates that the system cannot determine the state of the service, as indicated in the Critical Services pane.

For More Information

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

Adding RTMT Performance Counters in Bulk

On the RTMT Perfmon Monitoring pane, in table format only (not in chart format), you can now select multiple counters and multiple instances of counters, and add them all with a single click. Prior to this enhancement, you could add them only one at a time.

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

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 effect of the throttling slows the operations when IO utilization is in high demand for call processing, so that call processing can take precedence.

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

Trace Compression Support

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 that is required to store tracefiles.
- Reduces the disk head movement resulting in significantly improved disk I/O wait. This may be of value when tracefile demand is high.

For more information, see Documentation Updates, page 81.

CDR Analysis and Reporting Tool/Call Detail Record (CAR/CDR)

The following sections detail changes in CAR/CDR in release 6.1(1a) of Cisco Unified Communications Manager.

CAR System Scheduler Default Status

The CAR System Scheduler default status now specifies that CAR processes CDRs continuously 24 hours per day and 7 days per week. However, you can set the loading time, interval, and duration as needed. In addition, the default setting loads only CDR records. Call Management Records (CMR) records do not get loaded.

An option allows you to uncheck the “Load CDR Only” check box in the CAR System Scheduler window to allow CMR records to load.

Automatically Generated Reports

You can schedule CAR reports to generate automatically at a regular time. Each report that can be scheduled has its own report generation interval. In previous releases of Cisco Unified Communications Manager, the automatically generated reports default status specified **Enabled**. Beginning with Cisco Unified Communications Manager Release 6.1(1a), the default status specifies **Disabled** for the automatically generated reports. You must enable each automatically generated report after CAR is activated on your system.

Automatic E-Mail Alerts

For all new installations of Cisco Unified Communications Manager, you must enable the automatic e-mail alerts. The default status for all alerts specifies **Disabled**. In previous releases of Cisco Unified Communications Manager, the default status for all automatic e-mail alerts specified **Enabled**.

Tbl_pregenmail_option Table Data

For all Cisco Unified Communications Manager upgrades from Release 5.x to a later release of Cisco Unified Communications Manager, the tbl_pregenmail_option table data migrates only if the CAR Scheduler service is active.

Calculation of the Utilization of H.323 Gateways

For calculation of the utilization of H.323 gateways, the system uses the port numbers from the CAR Gateway Configuration window. To find this window, choose **System > System Parameters > Gateway Configuration**. You cannot take port details for H.323 gateways from the Cisco Unified Communications Manager database because the H.323 port number always equals zero in the database. The user must update H.323 gateway ports information in the CAR Gateway Configuration window.

Be aware that the only port detail information that is taken from the CAR Gateway Configuration window is for those gateways that do not have port details that are available or that show zero in the Cisco Unified Communications Manager database.

CDR Search Reports Display Time in Two Ways

The CDR Search by User Extension, CDR Search by Gateway, CDR Search by Call Precedence Levels, and CDR Search for Malicious Calls reports now display current time in both Coordinated Universal Time (UTC) and local time and use the following rules:

- The UTC and local time comprise a numeric string of mmddyyyy hhmmss, as in January 15, 2007 12:00:00.
- The default FromDate and ToDate values display in UTC.
- The default ToDate specifies the current time of the server in UTC.
- The default FromDate value specifies the ToDate value minus 1 hour. For example, if ToDate = January 15, 2007 12:00:00, the FromDate default value = January 15, 2007 11:00:00 (all times in UTC).

CAR Scheduler Now a Network Service

Installed automatically, network services include services that the Cisco Unified Communications Manager Business edition system requires to function. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. Cisco CAR Scheduler now represents a network service. In the previous release of Cisco Unified Communications Manager Business Edition the Cisco CAR Scheduler represented a feature service.

Cisco Unified Communications Manager User Options

The following enhancements occurred in the Cisco Unified CM User Options Menu (referred to as User Options) in release 6.1.

Call Forward

This section contains information on updates to the Cisco Unified CM User Options, Call Forward feature. Previous to release 6.1, users had only the Call Forward All option.

The Cisco Unified Communications Manager administrator determines the call forwarding options that are available to all users. From the Enterprise Parameters Configuration window, in the Show Call Forwarding field, the administrator chooses one of these options:

- Show All Settings
- Hide All Settings
- Show Only Forward All

From the Cisco Unified CM User Options window, users can configure the call forward all, call forward busy, call forward no answer, and call forward no coverage user options. To set the call forward user option, the user chooses **User Options > Device** and then clicks the Line Settings button. Users configure incoming external or internal calls to either a phone number or to a voice-messaging number.

Cisco Unified IP Phones

This section provides the following information:

- Cisco Unified IP Phone 7975G, page 53

Cisco Unified IP Phone 7975G

The Cisco Unified IP Phone 7975G is a full-feature IP-based phone that demonstrates the latest advances in VoIP telephony.

The Cisco Unified IP Phone 7975G extends the functionality of the existing Cisco Unified IP Phone 7970G and 7971G-GE models with the following features:

- A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection.
- High-fidelity audio for vibrant, life-like conversations; Internet Low Bitrate Codec (iLBC) support for use in lossy networks
- Gigabit Ethernet VoIP telephony technology
- Backlit, high-resolution, color touchscreen for easy access to communications information, XML applications, and features
- Access to eight telephone lines (or combination of lines, speed dials, and direct access to telephony features), five interactive soft keys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster.
- Integrated Ethernet switch and 10/100/1000BASE-T Ethernet connection via an RJ-45 interface for LAN connectivity
- Support for IEEE 802.3af Power (Class 3) over Ethernet (PoE) or a local power supply
- Standards-compliant SIP phone support

Requirements:

The Cisco Unified IP Phone 7975G requires one of the following releases at minimum:

- Cisco Unified Communications Manager 4.1(3)sr5b, 4.2(3)sr2b, 4.3(1), 5.1(1)b, 5.1(2), or 6.0(1).
- Cisco Unified Communications Manager Express Version 4.1 and Cisco IOS® Software Release 12.4(15)T.

Cisco Unified IP Phone 7965G and 7945G

The Cisco Unified IP Phone 7965G and 7945G is a full-feature IP-based phone that demonstrates the latest advances in VoIP telephony.

The Cisco Unified IP Phone 7965G and 7945G extend the functionality of the existing Cisco Unified IP Phone 7961G, 7961G-GE, 7941G, 7941G-GE models with the following features:

- High-fidelity audio for vibrant, life-like conversations; Internet Low Bitrate Codec (iLBC) support for use in lossy networks
- A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection.
- Gigabit Ethernet VoIP telephony technology
- Higher-resolution color display supports advanced XML applications
- Supports IEEE 803.af PoE (Class 3)or local power supply
- The Cisco Unified IP Phone 7965G provides access to six phone lines (or combination of lines, speed dials, and direct access to telephony features)
- The Cisco Unified IP Phone 7945G provides access to two phone lines (or combination of line access and direct access to telephony features)
- Four interactive soft keys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster.
- Integrated Ethernet switch and 10/100/100BASE-T Ethernet connection via an RJ-45 interface for LAN connectivity
- Standards-based
- Standards-compliant SIP phone support

Requirements:

The Cisco Unified IP Phone 7965G and 7945G requires one of the following releases at minimum:

- Cisco Unified Communications Manager 4.1(3)sr5b, 4.2(3)sr2b, 4.3(1), 5.1(1)b, 5.1(2), or 6.0(1).
- Cisco Unified Communications Manager Express Version 4.1 and Cisco IOS® Software Release 12.4(15)T.

Cisco Unified IP Phone 7962G and 7942G

The Cisco Unified IP Phone 7962G and 7942G extends the features and functionality of the existing Cisco Unified IP Phone 7961G and 7942G while enhancing the telephone user experience with the following features:

- High-fidelity wideband audio for lifelike conversations; Internet Low Bitrate Codec (iLBC) support for use in lossy networks
- High-resolution grayscale display for easy use of Cisco Unified Communications and third-party telephone applications
- Supports IEEE 803.af PoE (Class 2) or local power supply
- The Cisco Unified IP Phone 7962G provides access to six phone lines (or combination of lines and telephony features)
- The Cisco Unified IP Phone 7942G provides access to two phone lines (or combination of line access and telephony features)
- Integrated Ethernet switch and 10/100BASE-T Ethernet connection via an RJ-45 interface for LAN connectivity
- Standards-based
- Standards-compliant SIP phone support

Requirements:

The Cisco Unified IP Phone 7962G and 7942G requires one of the following releases at minimum:

- Cisco Unified Communications Manager 4.1(3)sr5b, 4.2(3)sr2b, 4.3(1), 5.1(1)b, 5.1(2), or 6.0(1).
- Cisco Unified Communications Manager Express Version 4.1 and Cisco IOS® Software Release 12.4(15)T.

Cisco Unified IP Conference Station 7937G

The Cisco Unified IP Conference Station 7937G, a full-feature IP-based conference station, allows you to place and receive calls, put calls on hold, transfer calls, make conference calls, and to access features such as mute, speed dial, call forward, and more.

Cisco Unified IP Conference Station 7937G for firmware release 1.0(1) provides support for the following features:

- Power over Ethernet (PoE) power that is provided by a switch through the Ethernet cable that is attached to the conference station
- Third-party lapel microphone kit that allows speakers to move around the conference room and still be easily heard
- Four softkey buttons that allow you to quickly access conference station features
- Expanded room coverage up to 30 feet by 40 feet with the optional external microphone kit
- Global language support

Note Be aware that Cisco Unified IP Conference Station 7937G is compatible with Cisco Unified Communications Manager, Releases 4.1, 4.2, 4.3, 5.1, 6.0, and later.

Connection Monitor

Connection Monitor enables an administrator to change the time that a link between a phone, which is registered with an SRST due to a failover, and a Cisco Unified Communications Manager must remain stable (with no link-flapping) before the phone falls back from SRST to the Cisco Unified Communications Manager.

Define the connection monitor duration in Cisco Unified Communications Manager Administration by using **System > Device Pool**. It applies to all IP phones in a specific device pool. The default value specifies 120 seconds.

Supported Cisco Unified IP Phones (SCCP and SIP)

7962G, 7942G, 7975G, 7965G, 7945G, 7970G, 7970G-GE, 7971G, 7971G-GE, 7906G, 7911G, 7931G (SCCP only), 7940G, 7960G

Intercom with Cisco Extension Mobility

Cisco Unified Communications Manager Release 6.1 supports the intercom feature for Cisco Extension Mobility users.

You must configure the following information for intercom:

- When you are configuring an intercom line, you must specify a default device in the Intercom Directory Number Configuration window. This applies regardless of whether the user will be using intercom with Cisco Extension Mobility. Be aware that the intercom line will be active only on the default device.
- Assign the phone button template that contains the intercom configuration to one (but not both) of the following items:
  - A specific device (Select the Intercom check box on the Device Configuration window.)
  - A user Extension Mobility profile (Select the Intercom check box on the profile.)

Note If a user logs into the same phone on a daily basis by using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile as opposed to a device.

For more information, refer to *Cisco Unified Communications Manager Features and Services Guide, Release 6.1*, Intercom chapter.

Supported Cisco Unified IP Phones (SCCP and SIP)

7975G, 7971G-GE, 7970G, 7965G, 7962G, 7961G-GE, 7961G, 7945G, 7942G, 7941G-GE, 7941G, 7931G (SCCP only)

Single Button Barge (SCCP)

When single button barge (SBB) is enabled, and when one call exists on the shared line, a user can barge by pressing the line key that corresponds to the call. To enable SBB, choose the applicable setting from the Single Button Barge drop-down list box that is on the Phone Configuration window.

If more than one call exists on the line or if SBB is not enabled, the user must highlight the call and press the Barge or cBarge softkey instead.

Supported Cisco Unified IP Phones (SCCP only)

7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G and G-GE, 7975G

Join Across Lines (SCCP)

Join allows a user to join and combine existing calls into a conference. Previous to release 6.1, Join required that calls be on the same line.

Join Across Lines (JAL) allows a user to join calls that are on multiple lines (either on different DNs, or on the same DN but on different partitions).

To enable JAL, choose the applicable setting from the Join Across Lines drop-down list box that is on the Phone Configuration window.

Supported Cisco Unified IP Phones (SCCP only)

7931G, 7940G, 7960G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G and G-GE, 7975G

Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1 Features

Table 4 lists Cisco Unified IP Phones that support new Cisco Unified Communications Manager 6.1 features.

Table 4 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1 Features

Cisco Unified Communications Manager 6.1 Feature	Cisco Unified IP Phone Support	For more information, see
Join Across Lines	SCCP only: 7975G 7971G-GE 7970G 7961G-GE 7941G-GE 7962G 7942G 7965G 7945G 7960G 7940G 7931G	Join Across Lines (SCCP), page 56
Intercom with Extension Mobility	SCCP and SIP: 7975G 7971G-GE 7970G 7961G-GE 7941G-GE 7942G 7962G 7945G 7965G SCCP only: 7931G	Intercom with Cisco Extension Mobility, page 55
Single Button Barge	SCCP only: 7975G 7971G-GE 7970G 7961G-GE 7941G-GE 7962G 7942G 7965G 7945G	Single Button Barge (SCCP), page 56

Cisco and Third-Party APIs

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

Cisco Unified TAPI

The following sections provide information about Cisco Unified TAPI for Cisco Unified Communications Manager Release 6.1(1a). Refer to *Cisco Unified TAPI Developers Guide* for additional information about Cisco Unified TAPI.

New Features

The following new features apply.

TSP Intercom Support with Extension Mobility

- Device profiles can include intercom lines.
- Log in by using Extension Mobility can include intercom lines
- LINE_CREATE/LINE_REMOVE for intercom lines with Extension Mobility
- Same intercom functionality on Extension Mobility intercom lines

TSP Product Security Incident Response Team (PSIRT) Enhancements

- Same passphrase on every machine changed to having a unique passphrase on every machine
- No changes to functionality or API

TSP Join Across Lines

- This feature allows two or more calls on different lines of the same device to be joined through the join operation.
- Applications can use the existing join API to perform the task.
- When the join across line happens, the consultation call on the line on which the survival call does not reside gets cleared, and a CONFERENCED call that represents the consultation call gets created on the primary line where conference parent gets created.
- This feature supports chaining of conference calls on different lines on the same device.
- You can perform a join across line on a non-controller line.
- This feature returns an error if one of the lines that is involved in the Join Across Lines is an intercom line.
- This feature gets supported on SCCP devices that CTI can control.

TSP Vista Support

- TSP supports the Microsoft Vista operating system
- When you use the Vista operating system, be aware of the following issues:

- Ensure a first-time installation of the CiscoTSP and Cisco Unified Communication Manager TSP Wave driver on a computer that is running the Vista operating system is performed as a fresh install.
- If a secure connection to Cisco Unified Communication Manager is used, turn off the Windows firewall.
- If the Cisco Unified Communication Manager TSP Wave driver is used for inbound audio streaming, turn off the Windows firewall.
- If the Cisco Unified Communication Manager TSP Wave driver is used for audio streaming, disable all other devices in the "Sound, video and game controllers" group.

Backward Compatibility Overview

No backward compatibility issue exists for all features that are introduced in 6.0 release if the feature is not used

Join Across Lines Use Case

This section provides an example of the join across lines functionality.

Action	Expected Event
A -> B1 is HOLD, C-> B2 is connected	For A: LINE_CALLSTATE param1=x100, CONNECTED Caller = A, Called = B1 Connected B1 For B1: LINE_CALLSTATE param1=x100, HOLD Caller = A, Called = B1, Connected = A For B2: LINE_CALLSTATE param1=x100, CONNECTED Caller = C, Called = B2, Connected = C For C: LINE_CALLSTATE param1=x100, CONNECTED Caller = C, Called = B2, Connected = B2

Action	Expected Event
Application issues lineDevSpecific(SLDST_JOIN) with the call on B1 as survival call	For A: CONNECTED CONFERENCED Caller=A, Called=B1, Connected=B1 CONFERENCED Caller=A Called=C, Connected=C For B1: CONNECTED CONFERENCED Caller=A, Called=B1, Connected=A CONFERENCED Caller=B1 Called=C, Connected=C For B2: Call will go IDLE For C: CONNECTED CONFERENCED Caller=C, Called=B2, Connected=B1 CONFERENCED Caller=C Called=A, Connected=A

Cisco Unified JTAPI

The following sections provide information about Cisco Unified JTAPI for Cisco Unified Communications Manager Release 6.1(1a). Refer to *Cisco Unified JTAPI Developers Guide* for related information about Cisco Unified JTAPI.

- New Features, page 60
- Backward Compatibility Issues, page 62
- Backward Compatibility Issues, page 62

New Features

These new features apply.

Certificate Download API Enhancement

New certificate download APIs provide increased security. New APIs require applications to specify a certificate passphrase, which is used to encrypt the java key store where client/server certificates are stored.

The system deprecates old certificate download APIs but they are still supported to avoid backward compatibility issue for applications. Cisco strongly recommends that applications migrate to the new APIs.

JTAPI also provides new API deleteCertificate() and deleteSecurityPropertyForInstance(), which applications can use to delete certificates that are already installed. To change passphrase for the certificate java key store, an application must delete the old certificate by using this API and upload the new certificate.

The enhanced JTAPI Preferences security tab provides two new buttons:

- **Delete Certificate**—Allows users to delete a certificate for the required user name/instanceID.
- **Update Certificate**—Allow users to upload certificate from the CAPF server. If the certificate update is successful, the certificate update dialog box displays Updated. In addition, the authorization string and certificate passphrase get cleared. If certificate update fails, the certificate dialog box continues to show a status of Not updated, unless the certificate was already updated. A user or applications must provide a certificate passphrase every time that an attempt is made to update a certificate. For security reasons, JTAPI does not save the certificate passphrase. An application must secure the passphrase and provide it through API when needed.

Be aware that this feature is compatible with previous releases of Cisco Unified Communications Manager.

Join Across Lines

The join across lines feature allows support for conferences across lines. It allows two or more calls on different addresses of the same terminal to be joined though the **Join** softkey on a Cisco Unified IP Phone or through the conference() API that JTAPI provides.

The behavior to JTAPI applications will change from previous releases because applications will not see a common controller in final and consult calls. No change occurs in the API, and same events get delivered whether calls are conferenced on the same address (regular conference) or across addresses (join across lines). When the join across lines feature is performed, CiscoConferenceStartEv/EndEv gets provided to all addresses on the controller terminal that have consult or final calls that are being joined into one conference. In CiscoConferenceStartEv, the conferenceControllerAddress always represents the primary controller address.

An application can set the controller via the setConferenceController() API. If an application does not specify this information, JTAPI itself finds a suitable controller for the conference. However, CIsco recommends that applications set the controller address when the join across lines feature is invoked. If an observer is not added on the controller address, applications may see null values for the talking or held terminal connection values in the CiscoConferenceStartEv.

With this release, the enhanced conference() API implementation means that all requests pass through after finding suitable terminal connections of the final and consult calls. JTAPI relies on the common terminal of the addresses that are involved in the call to find suitable terminal connections.

The system also supports multiple conference across address when more than two calls need to be joined.

SIP devices do not support this feature. JTAPI throws the exception (ILLEGAL_HANDLE) if this feature is requested on a SIP device.

You can disable this feature, which is backward compatible, by turning off the Join Across Lines Policy service parameter while Conference Chaining. You can disable the feature to allow a non-controller to add a participant to a conference by disabling the Advanced Ad Hoc Conference Enabled and Non-linear Ad Hoc Conference Linking Enabled service parameters.

Intercom Support for Extension Mobility

This enhancement provides support for the intercom feature for Extension Mobility while maintaining the single destination, non-sharable nature of intercom addresses. It requires intercom addresses to be configured with default terminal and allows configuring of intercom address on an Extension Mobility profile. When a user logs in to a terminal with an Extension Mobility profile that is configured with an intercom address, the system makes the intercom address available only if the default terminal of the intercom address is the same as the terminal where user logged in.

If an intercom address is configured on a terminal but the default terminal for the intercom address is not that terminal, the intercom address does not appear on the terminal. If this terminal is configured in the control list of JTAPI application, JTAPI does not create the intercom address in the provider domain.

From JTAPI point of view, no need exists for new interface or changes to support this feature. This feature, however, introduces some transitional scenarios in which the intercom functionary may not work on intercom addresses.

Consider this feature as compatible with previous releases of Cisco Unified Communications Manager.

Backward Compatibility Issues

This release of JTAPI is backward compatible with applications that are written for Cisco Unified Communications Manager 6.0.

Consider upgrading CiscoJtapiClient as not mandatory. Be aware that applications are required upgrade to Cisco Unified Communications Manager 6.1 CiscoJTAPIClient only if it is using any new features that are provided in this release.

Cisco Unified Communications Manager Configuration XML

The following sections provide information about Communications Manager Release 6.1(1a) XML. Refer to *Cisco Unified Communications Manager XML Developers Guide for Release 6.0(1)* for related information.

Documentation Updates

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
```

Added and Changed APIs

Cisco Unified Communications Manager 6.1 adds no new calls..

Table 5 describes the API calls that changed from the previous release. These changes might require updates to existing user code in which a changed feature is used.

Table 5 Changed API Calls

API Call	Remarks
addLine	Added new optional tag called defaultActivatedDevice for addLine API for Intercom CTI Support feature.
updateLine	Added new optional tag called defaultActivatedDevice for updateLine API for Intercom CTI Support feature.
getLine	Added new optional tag called defaultActivatedDevice for getLine API for Intercom CTI Support feature.
addUser	Added new optional tag called primaryDevice for addUser API for Mobility user feature.
updateUser	Added new optional tag called primaryDevice for updateUser API for Mobility user feature.
getUser	Added new optional tag called primaryDevice for getUser API for Mobility user feature.
addDeviceProfile	Added new optional tags called singleButtonBarge and joinAcrossLines for addDevice API for SingleButtonBarge and JoinAcrossLines feature.
updateDeviceProfile	Added new optional tags called singleButtonBarge and joinAcrossLines for updateDevice API for SingleButtonBarge and JoinAcrossLines feature
getDeviceProfile	Added new optional tags called singleButtonBarge and joinAcrossLines for getDevice API for SingleButtonBarge and JoinAcrossLines feature.
addDevicePool	Added new optional tags called singleButtonBarge and joinAcrossLines for addDevicePool API for SingleButtonBarge and JoinAcrossLines feature.
updateDevicePool	Added new optional tags called singleButtonBarge and joinAcrossLines for updateDevicePool API for SingleButtonBarge and JoinAcrossLines feature.
getDevicePool	Added new optional tags called singleButtonBarge and joinAcrossLine for getDevicePool API for SingleButtonBarge and JoinAcrossLines feature.

Table 5 Changed API Calls (continued)

API Call	Remarks
addPhone	Added new optional tags called singleButtonBarge and joinAcrossLines for SingleButtonBarge and JoinAcrossLines feature. The release adds “isActive” optional tag i for BAT/TAPS Licensing Allowance feature.
updatePhone	Added new optional tags called singleButtonBarge and joinAcrossLines for SingleButtonBarge and JoinAcrossLines feature. The release adds “isActive” optional tag for BAT/TAPS Licensing Allowance feature.
getPhone	Added new optional tags called singleButtonBarge and joinAcrossLines for SingleButtonBarge and JoinAcrossLines feature. The release adds “isActive” optional tag for BAT/TAPS Licensing Allowance feature.

Backward Compatibility Issues

Be aware that all Cisco Unified Communications Manager 6.0 AXL methods, with the exception of ExecuteSQLQuery and ExecuteSQLupdate, are backward compatible with Cisco Unified Communications Manager 6.1. By default, the interface automatically uses the 6.0 AXL schema. Developers should specify SOAPAction: “CUCM:DB ver=6.1” in the HTTP header to use any new 6.1 methods.

AXL Database APIs

Find detailed information for each method below in the *Cisco Unified Communications Manager AXL-SOAP API Documentation - v6.0(1) Interface Specification*, which is available at Cisco Developer Services:

http://www.cisco.com/cgi-bin/dev_support/access_level/product_support

Table 6 provides information about the AXL database APIs. This table includes these designations:

- M—Modified
- S—Supported
- X—Not supported

Table 6 AXL Database APIs

	Cisco Unified Communications Release											
Operation	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1	UCR[1]	Description
addAARGroup	X	X	X	S	S	X	X	X	S	S	S	
removeAARGroup	X	X	X	S	S	X	X	X	S	S	S	
updateAARGroup	X	X	X	S	S	X	X	X	S	S	S	
getAARGroup	X	X	X	S	S	X	X	X	S	S	S	
updateAARGroupMatrix	X	X	X	S	S	X	X	X	S	S	S	
listAARGroupByName	S	S	S	S	S	S	S	S	S	S	S	
addApplicationToSoftkeyTemplate	X	X	X	S	S	X	X	X	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
removeApplicationToSoftkeyTemplate	X	X	X	S	S	X	X	X	S	S	S	
updateAppUser	X	X	X	X	X	S	S	S	M	S	S	
addAttendantConsoleHuntGroup	X	X	X	S	S	S	S	S	S	S	S	
removeAttendantConsoleHuntGroup	X	X	X	S	S	S	S	S	S	S	S	
updateAttendantConsoleHuntGroup	X	X	X	S	S	M	S	S	S	S	S	
getAttendantConsoleHuntGroup	X	X	X	S	S	S	S	S	S	S	S	
addAttendantConsoleUser	X	X	X	S	S	S	S	S	S	S	S	
removeAttendantConsoleUser	X	X	X	S	S	S	S	S	S	S	S	
updateAttendantConsoleUser	X	X	X	S	S	S	S	S	S	S	S	
getAttendantConsoleUser	X	X	X	S	S	S	S	S	S	S	S	
addCalledPartyTransformationPattern	X	X	X	X	X	X	X	X	X	X	S	
removeCalledPartyTransformationPattern	X	X	X	X	X	X	X	X	X	X	S	
updateCalledPartyTransformationPattern	X	X	X	X	X	X	X	X	X	X	S	
getCalledPartyTransformationPattern	X	X	X	X	X	X	X	X	X	X	S	
addCallerFilterList	X	X	X	X	X	X	X	X	S	S	S	
removeCallerFilterList	X	X	X	X	X	X	X	X	S	S	S	
updateCallerFilterList	X	X	X	X	X	X	X	X	S	S	S	
getCallerFilterList	X	X	X	X	X	X	X	X	S	S	S	
addCallManager	S	S	S	S	S	M	S	S	S	S	S	
removeCallManager	S	S	S	S	S	S	S	S	S	S	S	
updateCallManager	S	S	S	S	S	M	S	S	S	S	S	
getCallManager	S	S	S	S	S	M	S	S	S	S	S	
addCallManagerGroup	S	S	S	S	S	S	S	S	S	S	S	
removeCallManagerGroup	S	S	S	S	S	S	S	S	S	S	S	
updateCallManagerGroup	S	S	S	S	S	S	S	S	S	S	S	
getCallManagerGroup	S	S	S	S	S	S	S	S	S	S	S	
addCallPark	S	S	S	S	S	M	S	S	S	S	S	
removeCallPark	S	S	S	S	S	S	S	S	S	S	S	
updateCallPark	S	S	S	S	S	S	S	S	S	S	S	
getCallPark	S	S	S	S	S	S	S	S	S	S	S	
addCallPickupGroup	S	S	S	S	S	S	S	S	M	S	S	
removeCallPickupGroup	S	S	S	S	S	S	S	S	S	S	S	
updateCallPickupGroup	S	S	S	S	S	S	S	S	M	S	S	
getCallPickupGroup	S	S	S	S	S	S	S	S	M	S	S	
getCCMVersion	X	X	X	X	X	X	X	X	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
addCMCInfo	X	X	S	S	S	S	S	S	S	S	S	
removeCMCInfo	X	X	S	S	S	S	S	S	S	S	S	
updateCMCInfo	X	X	S	S	S	S	S	S	S	S	S	
getCMCInfo	X	X	S	S	S	S	S	S	S	S	S	
addCommonDeviceConfig	X	X	X	X	X	X	X	X	S	S	M	
removeCommonDeviceConfig	X	X	X	X	X	X	X	X	S	S	S	
updateCommonDeviceConfig	X	X	X	X	X	X	X	X	S	S	M	
getCommonDeviceConfig	X	X	X	X	X	X	X	X	S	S	M	
addConferenceBridge	X	X	X	S	S	S	S	S	M	S	M	
removeConferenceBridge	X	X	X	S	S	S	S	S	S	S	S	
updateConferenceBridge	X	X	X	S	S	M	S	S	M	S	M	
getConferenceBridge	X	X	X	S	S	S	S	S	M	S	M	
addCredentialPolicy	X	X	X	X	X	X	X	X	S	S	S	
removeCredentialPolicy	X	X	X	X	X	X	X	X	S	S	S	
updateCredentialPolicy	X	X	X	X	X	X	X	X	S	S	S	
getCredentialPolicy	X	X	X	X	X	X	X	X	S	S	S	
addCSS	S	S	S	S	S	S	S	S	M	S	S	
removeCSS	S	S	S	S	S	S	S	S	S	S	S	
updateCSS	S	S	S	S	S	S	S	S	M	S	S	
getCSS	S	S	S	S	S	S	S	S	M	S	S	
listCSSByName	S	S	S	S	S	S	S	S	S	S	S	
addCTIRoutePoint	S	M	S	S	S	S	S	S	S	S	M	
removeCTIRoutePoint	S	S	S	S	S	S	S	S	S	S	S	
updateCTIRoutePoint	S	M	S	S	S	S	S	S	S	S	M	
getCTIRoutePoint	S	M	S	S	S	S	S	S	S	S	M	
addDDI	S	S	S	S	S	X	X	X	X	X	X	Use IDP to add DDI, DialPlan, and DialPlanTag.
removeDDI	S	S	S	S	S	X	X	X	X	X	X	Use IDP to add DDI, DialPlan, and DialPlanTag.
updateDDI	S	S	S	S	S	X	X	X	X	X	X	Use IDP to add DDI, DialPlan, and DialPlanTag.
getDDI	S	S	S	S	S	S	S	S	S	S	S	
addDeviceMobility	X	X	X	S	S	X	X	X	S	S	S	
removeDeviceMobility	X	X	X	S	S	X	X	X	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
updateDeviceMobility	X	X	X	S	S	X	X	X	S	S	S	
getDeviceMobility	X	X	X	S	S	X	X	X	S	S	S	
addDeviceMobilityGroup	X	X	X	S	S	X	X	X	S	S	S	
removeDeviceMobilityGroup	X	X	X	S	S	X	X	X	S	S	S	
updateDeviceMobilityGroup	X	X	X	S	S	X	X	X	S	S	S	
getDeviceMobilityGroup	X	X	X	S	S	X	X	X	S	S	S	
addDeviceProfile	S	M	M	S	S	S	S	M	M	M	S	
removeDeviceProfile	S	S	S	S	S	S	S	S	S	S	S	
updateDeviceProfile	S	M	M	S	S	M	S	M	M	M	S	
getDeviceProfile	S	M	M	S	S	S	S	M	M	M	S	
addDevicePool	S	M	S	M	S	M	S	M	M	M	M	
removeDevicePool	S	S	S	S	S	S	S	S	S	S	S	
updateDevicePool	S	M	S	M	S	M	S	M	M	M	M	
getDevicePool	S	M	S	S	S	S	S	M	M	M	M	
listDevicePoolByName	S	S	S	S	S	S	S	S	S	S	S	
addDialPlan	S	S	S	S	S	X	X	X	X	X	X	Use IDP to add DDI, DialPlan, and DialPlanTag.
removeDialPlan	S	S	S	S	S	X	X	X	X	X	X	Use IDP to remove DDI, DialPlan, and DialPlanTag.
updateDialPlan	S	S	S	S	S	X	X	X	X	X	X	Use IDP to update DDI, DialPlan, and DialPlanTag.
getDialPlan	S	S	S	S	S	S	S	S	S	S	S	
addDialPlanTag	S	S	S	S	S	X	X	X	X	X	X	Use IDP to add DDI, DialPlan, and DialPlanTag.
removeDialPlanTag	S	S	S	S	S	X	X	X	X	X	X	Use IDP to remove DDI, DialPlan, and DialPlanTag.
updateDialPlanTag	S	S	S	S	S	X	X	X	X	X	X	Use IDP to update DDI, DialPlan, and DialPlanTag.
getDialPlanTag	S	S	S	S	S	S	S	S	S	S	S	
addDirectedCallPark	X	X	X	S	S	X	X	X	S	S	S	
removeDirectedCallPark	X	X	X	S	S	X	X	X	S	S	S	
updateDirectedCallPark	X	X	X	S	S	X	X	X	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
getDirectedCallPark	X	X	X	S	S	X	X	X	S	S	S	
addFACInfo	X	X	S	S	S	S	S	S	S	S	S	
removeFACInfo	X	X	S	S	S	S	S	S	S	S	S	
updateFACInfo	X	X	S	S	S	S	S	S	S	S	S	
getFACInfo	X	X	S	S	S	S	S	S	S	S	S	
addGatekeeper	X	S	S	S	S	S	S	S	S	S	S	
removeGatekeeper	X	S	S	S	S	S	S	S	S	S	S	
updateGatekeeper	X	S	S	S	S	S	S	S	S	S	S	
getGatekeeper	X	S	S	S	S	S	S	S	S	S	S	
listGatekeeperByName	X	S	S	S	S	S	S	S	S	S	S	
addGatewayEndpoint	S	M	M	S	S	M	S	S	M	S	M	
removeGatewayEndpoint	S	S	S	S	S	S	S	S	S	S	S	
updateGatewayEndpoint	S	M	M	S	S	M	S	S	M	S	M	
getGatewayEndpoint	S	M	M	S	S	M	S	S	M	S	M	
addH323Gateway	X	S	M	S	S	M	S	S	S	S	M	
removeH323Gateway	X	S	M	S	S	S	S	S	S	S	S	
updateH323Gateway	X	S	M	S	M	M	S	S	S	S	S	
getH323Gateway	X	S	M	S	S	M	S	S	S	S	M	
addH323Phone	X	S	M	S	S	M	S	M	M	S	M	
removeH323Phone	X	S	M	S	S	S	S	S	S	S	S	
updateH323Phone	X	S	M	S	M	S	S	M	M	S	M	
getH323Phone	X	S	M	S	S	S	S	M	M	S	M	
addH323Trunk	X	S	M	S	S	S	S	S	M	S	M	
removeH323Trunk	X	S	M	S	S	S	S	S	S	S	S	
updateH323Trunk	X	S	M	S	M	S	S	S	M	S	M	
getH323Trunk	X	S	M	S	S	M	S	S	M	S	M	
addHuntList	X	X	S	S	S	M	S	S	S	S	S	
removeHuntList	X	X	S	S	S	S	S	S	S	S	S	
updateHuntList	X	X	S	S	S	M	S	S	S	S	S	
getHuntList	X	X	S	S	S	M	S	S	S	S	S	
addHuntPilot	X	X	S	S	S	S	S	S	S	S	M	
removeHuntPilot	X	X	S	S	S	S	S	S	S	S	S	
updateHuntPilot	X	X	S	S	S	M	S	S	S	S	M	
getHuntPilot	X	X	S	S	S	S	S	S	S	S	M	
addIVRUserLocale	X	X	X	X	X	X	X	X	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
removeIVRUserLocale	X	X	X	X	X	X	X	X	S	S	S	
aupdateIVRUserLocale	X	X	X	X	X	X	X	X	S	S	S	
agetIVRUserLocale	X	X	X	X	X	X	X	X	S	S	S	
updateLicenseCapabilities	X	X	X	X	X	X	X	X	S	S	S	
getLicenseCapabilities	X	X	X	X	X	X	X	X	S	S	S	
addLine	S	M	M	M	S	S	S	S	M	M	S	
removeLine	S	S	S	S	S	S	S	S	S	S	S	
updateLine	S	M	M	M	S	M	S	S	M	M	S	
getLine	S	S	S	S	S	S	S	S	M	M	S	
addLineGroup	X	X	X	S	S	M	S	S	S	S	S	
removeLineGroup	X	X	X	S	S	M	S	S	S	S	S	
updateLineGroup	X	X	X	S	S	M	S	S	S	S	S	
getLineGroup	X	X	X	S	S	M	S	S	S	S	S	
addLocation	S	M	S	S	S	S	S	S	S	S	S	
removeLocation	S	S	S	S	S	S	S	S	S	S	S	
updateLocation	S	M	S	S	S	S	S	S	S	S	S	
getLocation	S	M	S	S	S	S	S	S	S	S	S	
listLocationByName	S	S	S	S	S	S	S	S	S	S	S	
addMediaResourceGroup	S	S	S	S	S	S	S	S	S	S	S	
removeMediaResourceGroup	S	S	S	S	S	S	S	S	S	S	S	
updateMediaResourceGroup	S	S	S	S	S	S	S	S	S	S	S	
getMediaResourceGroup	S	S	S	S	S	S	S	S	S	S	S	
listMediaResourceGroupByName	S	S	S	S	S	S	S	S	S	S	S	
addMediaResourceList	S	S	S	S	S	S	S	S	S	S	S	
removeMediaResourceList	S	S	S	S	S	S	S	S	S	S	S	
updateMediaResourceList	S	S	S	S	S	S	S	S	S	S	S	
getMediaResourceList	S	S	S	S	S	S	S	S	S	S	S	
addMeetMe	X	X	X	S	S	X	X	X	S	S	S	
removeMeetMe	X	X	X	S	S	X	X	X	S	S	S	
updateMeetMe	X	X	X	S	S	X	X	X	S	S	S	
getMeetMe	X	X	X	S	S	X	X	X	S	S	S	
listMediaResourceListByName	S	S	S	S	S	S	S	S	S	S	S	
addMGCP	S	S	S	S	S	S	S	S	M	S	S	MGCP represents the box level configuration for a gateway.
removeMGCP	S	S	S	S	S	S	S	S	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
updateMGCP	S	S	S	S	S	M	S	S	S	S	S	
getMGCP	S	S	S	S	S	S	S	S	M	S	S	
addMGCPEndpoint	S	M	S	S	S	M	S	S	S	S	M	MGCPEndpoint specifies the port on the gateway.
removeMGCPEndpoint	S	S	S	S	S	S	S	S	S	S	S	
addMGCPUnit	S	S	S	S	S	S	S	S	S	S	S	MGCPUnit specifies the gateway Network Module.
removeMGCPUnit	S	S	S	S	S	S	S	S	S	S	S	
addMGCPSubunit	S	S	S	S	S	S	S	S	S	S	S	MGCPSubunit specifies the gateway VIC or VWIC.
removeMGCPSubunit	S	S	S	S	S	S	S	S	S	S	S	
addMobileVoiceAccess	X	X	X	X	X	X	X	X	S	S	S	
removeMobileVoiceAccess	X	X	X	X	X	X	X	X	S	S	S	
updateMobileVoiceAccess	X	X	X	X	X	X	X	X	S	S	S	
getMobileVoiceAccess	X	X	X	X	X	X	X	X	S	S	S	
addMobility	X	X	X	X	X	X	X	X	S	S	S	
removeMobility	X	X	X	X	X	X	X	X	S	S	S	
updateMobility	X	X	X	X	X	X	X	X	S	S	S	
getMobility	X	X	X	X	X	X	X	X	S	S	S	
updateMOHAudioSource	S	S	S	S	S	S	S	S	S	S	S	
removeMOHAudioSource	S	S	S	S	S	S	S	S	S	S	S	Blanks out the MOHAudioSource as if it were removed.
getMOHAudioSource	S	S	S	S	S	S	S	S	S	S	S	
listMOHAudioSourceByName	S	S	S	S	S	S	S	S	S	S	S	
addMOHServer	X	X	X	S	S	X	X	X	S	S	M	
removeMOHServer	X	X	X	S	S	X	X	X	S	S	S	
updateMOHServer	X	X	X	S	S	X	X	X	S	S	M	
getMOHServer	X	X	X	S	S	X	X	X	S	S	M	
addPhone	S	M	M	S	S	M	S	M	M	M	M	
removePhone	S	S	S	S	S	S	S	S	S	S	S	
updatePhone	S	M	M	S	S	M	S	M	M	M	M	
getPhone	S	M	M	S	S	M	S	M	M	M	M	
listPhoneByDescription	S	S	S	S	S	S	S	S	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
listPhoneByName	S	S	S	S	S	S	S	S	S	S	S	
listPhoneTemplateByName	S	S	S	S	S	S	S	S	S	S	S	
addPhoneTemplate	X	X	X	S	S	X	X	X	S	S	S	
removePhoneTemplate	X	X	X	S	S	X	X	X	S	S	S	
updatePhoneTemplate	X	X	X	S	S	X	X	X	S	S	S	
getPhoneTemplate	X	X	X	S	S	X	X	X	S	S	S	
addPhysicalLocation	X	X	X	S	S	X	X	X	S	S	S	
removePhysicalLocation	X	X	X	S	S	X	X	X	S	S	S	
updatePhysicalLocation	X	X	X	S	S	X	X	X	S	S	S	
getPhysicalLocation	X	X	X	S	S	X	X	X	S	S	S	
addPilotPoint	X	X	S	S	S	M	S	S	S	S	S	
removePilotPoint	X	X	S	S	S	S	S	S	S	S	S	
updatePilotPoint	X	X	S	S	S	M	S	S	S	S	S	
getPilotPoint	X	X	S	S	S	M	S	S	S	S	S	
addProcessNode	S	S	M	S	S	S	S	S	S	S	M	
removeProcessNode	S	S	M	S	S	S	S	S	S	S	S	
updateProcessNode	S	S	M	S	S	S	S	S	S	S	M	
getProcessNode	S	S	M	S	S	S	S	S	S	S	M	
updateProcessNodeService	S	S	S	S	S	M	S	S	S	S	S	
getProcessNodeService	S	S	S	S	S	M	S	S	S	S	S	
listProcessNodesByService	S	S	M	S	S	S	S	S	S	S	S	
listAllProcessNodes	S	S	M	S	S	S	S	S	S	S	S	
addRecordingProfile	X	X	X	X	X	X	X	X	S	S	S	
removeRecordingProfile	X	X	X	X	X	X	X	X	S	S	S	
updateRecordingProfile	X	X	X	X	X	X	X	X	S	S	S	
getRecordingProfile	X	X	X	X	X	X	X	X	S	S	S	
addRegion	S	S	S	S	S	S	S	S	M	S	S	
removeRegion	S	S	S	S	S	S	S	S	S	S	S	
updateRegion	S	S	S	S	S	S	S	S	M	S	S	
getRegion	S	S	S	S	S	S	S	S	M	S	S	
updateRegionMatrix	S	M	S	S	S	S	S	S	M	S	S	
addRemoteDestination	X	X	X	X	X	X	X	X	S	S	M	
removeRemoteDestination	X	X	X	X	X	X	X	X	S	S	S	
updateRemoteDestination	X	X	X	X	X	X	X	X	S	S	M	
getRemoteDestination	X	X	X	X	X	X	X	X	S	S	M	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
addRemoteDestinationProfile	X	X	X	X	X	X	X	X	S	S	M	
removeRemoteDestinationProfile	X	X	X	X	X	X	X	X	S	S	S	
updateRemoteDestinationProfile	X	X	X	X	X	X	X	X	S	S	M	
getRemoteDestinationProfile	X	X	X	X	X	X	X	X	S	S	M	
updateResourcePriorityDefaultNamespace	X	X	X	X	X	X	X	X	X	X	S	
getResourcePriorityDefaultNamespace	X	X	X	X	X	X	X	X	X	X	S	
addResourcePriorityNamespace	X	X	X	X	X	X	X	X	X	X	S	
removeResourcePriorityNamespace	X	X	X	X	X	X	X	X	X	X	S	
updateResourcePriorityNamespace	X	X	X	X	X	X	X	X	X	X	S	
getResourcePriorityNamespace	X	X	X	X	X	X	X	X	X	X	S	
addResourcePriorityNamespaceList	X	X	X	X	X	X	X	X	X	X	S	
removeResourcePriorityNamespaceList	X	X	X	X	X	X	X	X	X	X	S	
updateResourcePriorityNamespaceList	X	X	X	X	X	X	X	X	X	X	S	
getResourcePriorityNamespaceList	X	X	X	X	X	X	X	X	X	X	S	
addSIPTrunkSecurityProfile	X	X	X	X	X	X	X	X	X	X	S	
removeSIPTrunkSecurityProfile	X	X	X	X	X	X	X	X	X	X	S	
updateSIPTrunkSecurityProfile	X	X	X	X	X	X	X	X	X	X	S	
getSIPTrunkSecurityProfile	X	X	X	X	X	X	X	X	X	X	S	
getMobileSmartClientProfile	X	X	X	X	X	X	X	X	X	X	S	
addRouteFilter	S	S	S	S	S	S	S	S	S	S	S	
removeRouteFilter	S	S	S	S	S	S	S	S	S	S	S	
updateRouteFilter	S	S	S	S	S	S	S	S	S	S	S	
getRouteFilter	S	S	S	S	S	S	S	S	S	S	S	
addRouteGroup	S	S	S	S	S	S	S	S	S	S	S	
removeRouteGroup	S	S	S	S	S	S	S	S	S	S	S	
updateRouteGroup	S	S	S	S	S	S	S	S	S	S	S	
getRouteGroup	S	S	S	S	S	S	S	S	S	S	S	
addRouteList	S	M	M	S	S	S	S	S	S	S	M	
removeRouteList	S	S	S	S	S	S	S	S	S	S	S	
updateRouteList	S	M	M	S	S	S	S	S	S	S	M	
getRouteList	S	M	M	S	S	S	S	S	S	S	M	
addRoutePartition	S	S	M	S	S	S	S	S	M	S	S	
removeRoutePartition	S	S	M	S	S	S	S	S	S	S	S	
updateRoutePartition	S	S	M	S	S	S	S	S	M	S	S	
getRoutePartition	S	S	M	S	S	S	S	S	M	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
listRoutePartitionByName	S	S	S	S	S	S	S	S	S	S	S	
addRoutePattern	S	M	M	S	M	M	S	S	S	S	M	
removeRoutePattern	S	S	S	S	S	S	S	S	S	S	S	
updateRoutePattern	S	M	M	S	M	M	S	S	S	S	M	
getRoutePattern	S	M	M	S	M	S	S	S	S	S	M	
listRoutePlanByType	S	S	S	S	S	S	S	S	S	S	S	
updateServiceParameter	S	S	S	S	S	M	S	S	S	S	S	
getServiceParameter	S	S	S	S	S	S	S	S	S	S	S	
listServiceParameters	S	S	S	S	S	S	S	S	S	S	S	
addSIPProfile	X	X	X	X	X	X	X	X	X	X	S	
removeSIPProfile	X	X	X	X	X	X	X	X	X	X	S	
updateSIPProfile	X	X	X	X	X	X	X	X	X	X	S	
getSIPProfile	X	X	X	X	X	X	X	X	X	X	S	
addSIPRealm	X	X	X	X	X	X	S	S	S	S	S	
removeSIPRealm	X	X	X	X	X	X	S	S	S	S	S	
updateSIPRealm	X	X	X	X	X	X	S	S	S	S	S	
getSIPRealm	X	X	X	X	X	X	S	S	S	S	S	
addSIPTrunk	X	X	S	S	S	M	S	S	M	S	M	
removeSIPTrunk	X	X	S	S	S	S	S	S	S	S	S	
updateSIPTrunk	X	X	S	S	S	M	S	S	M	S	M	
getSIPTrunk	X	X	S	S	S	M	S	S	M	S	M	
updateSoftKeySet	X	X	X	S	S	X	X	X	S	S	S	
getSoftKeySet	X	X	X	S	S	X	X	X	S	S	S	
addSoftKeyTemplate	X	X	X	S	S	X	X	X	S	S	S	
removeSoftKeyTemplate	X	X	X	S	S	X	X	X	S	S	S	
updateSoftKeyTemplate	X	X	X	S	S	X	X	X	S	S	S	
getSoftKeyTemplate	X	X	X	S	S	X	X	X	S	S	S	
addTimePeriod	X	X	S	S	S	S	S	S	S	S	M	
removeTimePeriod	X	X	S	S	S	S	S	S	S	S	S	
updateTimePeriod	X	X	S	S	S	S	S	S	S	S	M	
getTimePeriod	X	X	S	S	S	S	S	S	S	S	M	
addTimeSchedule	X	X	S	S	S	S	S	S	S	S	M	
removeTimeSchedule	X	X	S	S	S	S	S	S	S	S	S	
updateTimeSchedule	X	X	S	S	S	S	S	S	S	S	M	
getTimeSchedule	X	X	S	S	S	S	S	S	S	S	M	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
addTODAccess	X	X	X	X	X	X	X	X	X	X	S	
removeTODAccess	X	X	X	X	X	X	X	X	X	X	S	
updateTODAccess	X	X	X	X	X	X	X	X	X	X	S	
getTODAccess	X	X	X	X	X	X	X	X	X	X	S	
addTranscoder	X	X	X	S	S	X	X	X	S	S	M	
removeTranscoder	X	X	X	S	S	X	X	X	S	S	S	
updateTranscoder	X	X	X	S	S	X	X	X	S	S	M	
getTranscoder	X	X	X	S	S	X	X	X	S	S	M	
addTransformationPattern	X	X	X	X	X	X	X	X	S	S	M	For adding CallingPartyTransformationPattern
removeTransformationPattern	X	X	X	X	X	X	X	X	S	S	S	For removing CallingPartyTransformationPattern
updateTransformationPattern	X	X	X	X	X	X	X	X	S	S	M	For updating CallingPartyTransformationPattern
getTransformationPattern	X	X	X	X	X	X	X	X	S	S	M	For getting CallingPartyTransformationPattern
addTransPattern	S	M	S	S	S	S	S	S	S	S	M	
removeTransPattern	S	S	S	S	S	S	S	S	S	S	S	
updateTransPattern	S	M	S	S	S	M	S	S	S	S	M	
getTransPattern	S	M	S	S	S	S	S	S	S	S	M	
addUser	S	M	M	S	S	M	S	S	M	M	M	
removeUser	S	M	M	S	S	S	S	S	S	S	S	
updateUser	S	M	M	S	S	M	S	S	M	M	M	
getUser	S	M	S	S	S	M	S	S	M	M	M	
listUserByName	S	M	M	S	S	M	S	S	S	S	S	
addUserGroup	X	X	X	X	X	S	S	S	S	S	S	
removeUserGroup	X	X	X	X	X	S	S	S	S	S	S	
updateUserGroup	X	X	X	X	X	S	S	S	S	S	S	
getUserGroup	X	X	X	X	X	S	S	S	S	S	S	
addVoiceMailPilot	X	X	S	S	S	S	S	S	S	S	S	
removeVoiceMailPilot	X	X	S	S	S	S	S	S	S	S	S	
updateVoiceMailPilot	X	X	S	S	S	S	S	S	S	S	S	
getVoiceMailPilot	X	X	S	S	S	S	S	S	S	S	S	

Table 6 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR[1]	Description
	3.3	4.0	4.1	4.2	4.3	5.0 d	5.1	5.1(2)	6.0	6.1		
addVoiceMailPort	S	M	S	S	S	S	S	S	M	S	M	
removeVoiceMailPort	S	S	S	S	S	S	S	S	S	S	S	
updateVoiceMailPort	S	M	S	S	S	S	S	S	M	S	M	
getVoiceMailPort	S	M	S	S	S	S	S	S	M	S	M	
addVoiceMailProfile	X	X	S	S	S	S	S	S	S	S	S	
removeVoiceMailProfile	X	X	S	S	S	S	S	S	S	S	S	
updateVoiceMailProfile	X	X	S	S	S	S	S	S	S	S	S	
getVoiceMailProfile	X	X	S	S	S	S	S	S	S	S	S	
listVoiceMailProfileByName	S	S	S	S	S	S	S	S	S	S	S	
createAutogeneratedProfile	S	S	S	S	S	S	S	S	S	S	S	
doAuthenticateUser	X	X	X	X	X	S	S	S	S	S	S	
doDeviceLogin	S	S	S	S	S	S	S	S	S	S	S	
doDeviceLogout	S	S	S	S	S	M	S	S	S	S	S	
doDeviceReset	S	S	S	S	S	M	S	S	S	S	S	
executeSQLQuery	X	S	S	S	S	S	S	S	S	S	S	
executeSQLUpdate	X	X	X	X	X	S	S	S	S	S	S	
getNumDevices	S	S	S	S	S	S	S	S	S	S	S	
listDeviceByNameAndClass	S	S	S	S	S	S	S	S	S	S	S	

1. UCR = Under consideration or review.

Cisco Unified Communications Manager Serviceability XML

No changes occurred for Cisco Unified Communications Manager Serviceability XML from release 6.0, and no issues with backward compatibility exist.

Table 7 provides information about the Serviceability SOAP API. This table includes these designations:

- M—Modified
- S—Supported
- X—Not supported

Table 7 Serviceability SOAP API Details

SOAP Service	Operation	Cisco Unified Communications Manager Release						UCR[1]
		3.0	4.0	4.3	5.0	6.0	6.1	
RisPort (Real Time Information Port)	selectCmDevice	X	S	S	S	S	S	S
	selectCtiItem	X	S	S	S	S	S	S
	getServerInfo	X	X	X	S	S	S	S
	SelectCmDevice (new API)	X	X	X	X	X	X	S

Table 7 Serviceability SOAP API Details (continued)

SOAP Service	Operation	Cisco Unified Communications Manager Release						
		3.0	4.0	4.3	5.0	6.0	6.1	UCR[1]
PerfmonPort (Performance Information Port)	perfmonOpenSession	S	S	S	S	S	S	S
	perfmonAddCounter	S	S	S	S	S	S	S
	perfmonRemoveCounter	S	S	S	S	S	S	S
	perfmonCollectSessionData	S	S	S	S	S	S	S
	perfmonCloseSession	S	S	S	S	S	S	S
	perfmonListInstance	S	S	S	S	S	S	S
	perfmonQueryCounterDescription	S	S	S	S	S	S	S
	perfmonListCounter	S	S	S	S	S	S	S
	perfmonCollectCounterData	S	S	S	S	S	S	S
ControlCenterServicesPort (All Service Control APIs)	soapGetStaticServiceList	X	X	X	S	S	S	S
	soapGetServiceStatus	X	X	X	S	S	S	S
	soapDoServiceDeployment	X	X	X	S	S	S	S
	soapDoControlServices	X	X	X	S	S	S	S
	getProductInformationList	X	X	X	X	S	S	S
LogCollectionPort (All Log Collection APIs)	listNodeServiceLogs	X	X	X	S	S	S	S
	selectLogFiles	X	X	X	S	S	S	S
CDRonDemand (All CDR APIs)	get_file_list	X	X	X	S	S	S	S
	get_file	X	X	X	S	S	S	S
DimeGetFileService (Getting Single File)	GetOneFile	X	X	X	S	S	S	S

1. UCR = Under consideration or review.

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(1a) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

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

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

Table 8 describes possible unexpected behaviors in Cisco Unified Communications Manager Release 6.1(1b), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 6 to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the "First Fixed-in Version" or "Integrated-in" fields. The information that displays in these fields identifies the list of Cisco Unified Communications Manager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Communications Manager releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1. However, the version information that displays for the Cisco Unified Communications Manager maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco Unified Communications Manager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 005.000(000.123) = Cisco Unified Communications Manager Release 5.0(1)
- 005.000(001.008) = Cisco Unified Communications Manager Release 5.0(2)
- 005.001(002.201) = Cisco Unified Communications Manager Release 5.1(3)
- 006.000(000.123) = Cisco Unified Communications Manager Release 6.0(1)

Note Because defect status continually changes, be aware that Table 8 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 77.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Table 8 Open Caveats as of April 7, 2008

Identifier	Headline
Component: Attendent Console	
CSCso42789	AC migrator throws Java exception errors.
Component: AXL	
CSCso54610	AXL processes the request with wrong version specified in the request.
Component: CM Serviceability	
CSCsk96900	Unified CM SDI trace delete should be lower priority.
Component: CLI	
CSCso62779	CLI does not use RFC 1123 to verify hostnames for compliance.
Component: Unified CM Docs	
CSCsh86972	Need exists for an alternative for AAR to allow TEHO / toll bypass / GW calls.
Component: Unified CM CTI	

Table 8 Open Caveats as of April 7, 2008

CSCsl36547	CTI heartbeat timeout; provider closing.
CSCsm97805	Change Notification failure on Forward on CTI Failure field.
CSCsk93949	Don't get failure response when initiator park barged call on SIP phone
Component: Unified CM User Interface	
CSCso62160	Error on time settings page for subscriber server.
CSCso56349	If user changes to an unsupported RFC1123 hostname, no error displays.
Component: Call Processing	
CSCso28030	H323: Tandberg: H225D Line Control, Device Register messages for stopped session.
CSCso38061	Line Control: Phone plays BLF audible alert tone when monitoring DN does not alert.
CSCso45926	Line Control: EM login, phone does not register.
CSCsl04498	Media Control: When the Unity call handler completes a transfer, no audio exists on the IP phone.
CSCso53770	Media Control: Hold / resume to a third-party H.323 gateway fails intermittently.
CSCso44696	Media Control: MTP resource leak occurs on SIP trunk.
CSCso20569	Media Control: Unified CM cored during IPCC 15 hour traffic test .
CSCsi56627	Media Control: Need exists for transcoder allocation to be handled differently when H.323 ICT is involved.
CSCsm23539	Media Control: POC SIP SS DO-EO : Rinback not heard for XEE.
CSCso57477	MGCP: Voice path not cut through after disc with PI and overlap sending from H323.
CSCso55307	Mobility: Mobility internal number associated to RDP includes a prefix.
CSCsm70455	QSIG: Unified CM does not honor reroute request from Matra PBX.
CSCso62633	SCCP: CTI application cannot retrieve a call redirected between nodes.
CSCso42673	SCCP: DND does not respond in English-UK and French locales.
CSCsh97800	SCCP: Transfer cannot complete if phone answers an incoming call before the transfer completes.
CSCso27104	SIP: SIP Phone log park number gets placed in call history.
CSCsi27220	SIP Station: When barging a Cisco Unified IP Phone 7960, SCCP TNP ringout occurs for three minutes.
CSCso57197	SIP Station: User cannot cBarge into busy call.
CSCsm70395	SS-Callback: CCBS fails for Unified CM to Tenovis PBX; and Unified CM to Matra PBX.
CSCsm70225	SS-Callback: CCBS callback fails between Tenovis PBX and Unified CM; and Matra PBX and Unified CM.
CSCso51128	Subscriptioning: Call list presence does not work if directory sync contains a space in the DN.
CSCso14732	Supplementary Services: CF uses incorrect cause code (31 instead of 25) on loop detection
CSCsh36576	System: Signaling DSCP from Unified CM incorrect for CS5, CS6, CS7, EF.
CSCsk72804	System: CallManager project gets compiled without -Wall.

Table 8 Open Caveats as of April 7, 2008

CSCsm37511	System: Unified CM SDL trace files do not get deleted when the count gets modified.
CSCso15856	System: Virtual memory rising in the SJC Alpha Unified CM nodes.
CSCso51858	Unknown: Call routing does not follow the TimeofDay routing rules.
Component: CPI	
CSCsk29296	Appinstall: Unified CM 5.x installer prevents RFC 1123 for DNS compliant hostnames.
CSCso53944	Appinstall: Unified CM configuration after skip install fails during setup.
CSCso40870	Certificate Management: The CLI command **set web-security** does not delete the old CSR and regenerate a new one.
CSCsl71487	Operating System: RTMT and perfmon counters show cimserver process memory consumption increases.
CSCso61240	Platform API: ciscocm.CSCso53771.security.patch.cop.sgn stops At "Securing DRS Port".
CSCso57947	Platform API: Unified CM 6.x - GUI displays no error for COP file install problem.
CSCso57806	Platform API: Unified CM Release 6.1 software install prematurely shows "Status Complete", empty install log.
CSCso51380	Security: Scheduled trace collection remains in the "RUNNING" state, but no trace file get collected.
Component: Database	
CSCso20115	Database replication fails after subscriber server fresh install on cdr define.
CSCso47114	PMR 64860 - cdr check fail "Bad row id".
CSCsj78789	DMA validation fails with International Dial plans.
CSCso35247	Need exists for much faster database replication setup.
CSCso41720	PMR 44626 Replication setup failure occurs after upgrade ISAM error: deadlock.
CSCso60877	Replication state does not get updated.
CSCsm28295	Device table not in sync after 'utils dbreplication [reset - repair]'.
CSCso22817	Replication setup fails because cdr check does not delete extra rows.
CSCsm78505	Excessive database connections and memory usage exists.
CSCso13724	CredentialDynamic table contains mismatches after database replication setup completes.
Component: Directory	
CSCso30000	SSL LDAP authentication fails for Unified CM with AD 2003.
Component: JTAPI Dev Test	
CSCsk94127	Import dev-test tool to clearcase.
Component: JTAPI SDK	
CSCso44211	Configuration is successful even when there are two participants due to MTP failure.
Component: QED	
CSCsm81902	Need exists for additional devices for CTS500, CTS1000, CTS3000, CTS3200.
Component: QRT	

Table 8 Open Caveats as of April 7, 2008

CSCsk31721	When web access is disabled, problems do not get reported from the phone.
Component: RISDC	
CSCso58779	Immediately after an upgrade, RTMT reports an RIS DC core on the active partition.
Component: Real Time Monitoring Tool	
CSCsk78816	User cannot configure trace collection because RTMT trace collection menu items display an error when you select them.
Component: TabSync	
CSCso12859	TabSync authentication fails with Unified CM if password contains '+' character.
Component: TAPISDK	
CSCsl31067	No LINE_MONITORTONE returned RecordWave with silence- Vista.

Documentation Updates

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

Omissions

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Communications Manager 6.1(1x).

CAR Records Migration Issues

The Upgrading to Cisco Unified Communications Manager Release 6.1(1) from Cisco Unified CallManager 4.x Releases Guide and the Data Migration Assistant User Guide do not explain that Data Migration Assistant does not migrate CDR data except those records in the CAR database. If you generate CDRs after you have run CDR loader in CAR, DMA does not migrate those CDRs. For information on configuring the CAR load schedule before you upgrade, see the Cisco Unified CallManager Serviceability Administration Guide for the version of Cisco CallManager running on your system.

Make sure that you purge any CAR records older than 180 days. The version of CAR that runs on Cisco Unified Communications Manager 6.1(1) does not retain CDRs older than 180 days in the CAR database. If you migrate records older than 180 days, the system deletes them immediately after you upgrade. For information on configuring automatic database purging after you upgrade, refer to the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide for Cisco Unified Communications Manager.

The Cisco Unified Communications Manager installation program limits the time in which CAR records are migrated from the DMA TAR file to the CAR database on the upgraded system. The installer migrates approximately 100,000 to 150,000 of the oldest individual CAR records within the time limit. Any records that cannot be exported during the specified time will not be migrated.

Disaster Recovery Manual Backup Checkbox

The *Disaster Recovery System Administration Guide* for 6.0(1) does not mention that the Manual Backup window no longer contains a CAR/CDR checkbox and that Disaster Recovery System backs up CAR/CDR data automatically when you check the CCM checkbox on the Manual Backup window. The Disaster Recovery System Administration Guide for 6.0(1) supports the Cisco Unified Communications Manager 6.1(1) release.

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 is 30 days.

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.

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.

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.

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

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.)

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.

DNS Required for RTMT Alerts by E-mail

The *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* and the *Cisco Unified Serviceability 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.

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 that 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*

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, 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 SCCP phone, 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 SCCP phone, a new row for exists 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 SCCP phone,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 SCCP phone, 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.

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.

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.

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.

Errors

This section provides information about errors that exist in the Cisco Unified Communications Manager Release 6.1(1a) documentation.

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 is 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 CallManager:

/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 is 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 CallManager:

//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 CallManager.

Step 6 Power cycle the phone.

The new graphic displays when the phone restarts.

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**.

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* and the *Cisco Unified Communications Manager System Guide* suggest 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**.

Call Admission Control Bandwidth Example Correction

The Call Admission Control chapter of the *Cisco Unified Communications Manager System Guide* incorrectly describes the amount of bandwidth that is consumed in an example locations-type call admission control scenario.

Original explanation:

Cisco Unified Communications Manager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kbps of available bandwidth, that link can support one G.711 call at 80 kbps (in each direction), three G.723 or G.729 calls at 24 kbps each (in each direction), or two GSM calls at 29 kbps each (in each direction). If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone.

Correct explanation:

Cisco Unified Communications Manager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kbps of available bandwidth, that link can support two G.711 calls at 80 kbps each, six G.723 or G.729 calls at 24 kbps each, or five GSM calls at 29 kbps each. If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone

Barge and Security

The “Restrictions” section of the Barge and Privacy chapter in the *Cisco Unified Communications Manager Features and Services Guide* misstates the capabilities of encrypted phones to accept barge requests from unencrypted phones or from calls with a lower security level in Cisco Unified Communications Manager Release 6.1(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 Visual Indicator

The Cisco Unified IP Phone Configuration chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly states that a spinning circle on the phone display indicates that a barge is taking place. Only an audible indicator occurs.

Barge with Shared Conference Bridge

The Barge and Privacy chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not correctly describe the process for configuration of the Barge with Shared Conference Bridge feature. The Standard User and Standard Feature softkey templates do not support cBarge and cannot be modified. The following corrections apply to 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.

Adding an Administrator User to Cisco Unity or Cisco Unity Connection

The Application User chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can use the Create Cisco Unity Application User link in the Related Links drop-down list box to create an application user voice mailbox in Cisco Unity or Cisco Unity Connection. You use this link to add an administrator user to Cisco Unity or Cisco Unity Connection.

1. Correct the Next Steps section in "Configuring an Application User" section to read as follows:

   Next Steps

   If you want to associate devices with this application user, continue with the "Associating Devices to an Application User" procedure.

   To manage credentials for this application user, continue with the "Managing Application User Credential Information" procedure.

   To add this administrator user to Cisco Unity or Cisco Unity Connection, continue with the procedure in " Adding an Administrator User to Cisco Unity or Cisco Unity Connection" section on page 92.

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 "Finding an Application User" section.

Step 2 From the Related Links drop-down list box, in the upper, right corner of the window, choose the Create Cisco Unity Application User link and click **Go**.

The Add Cisco Unity User dialog box displays.

Step 3 From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click **Next**.

Step 4 From the Application User Template drop-down list box, choose the template that you want to use.

Step 5 Click **Save**.

The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to Edit Cisco Unity User in the Application User Configuration window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Note When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified Communications Manager Application User, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration), First Name, Last Name, Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Administration or Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Note Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration at the Tools menu. For Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* for more information. For Cisco Unity, refer to the *Cisco Unity System Administration Guide*.

Number of Alphanumeric Characters Allowed in the Pickup Group Name Field

The *Cisco Unified Communications Manager Features and Services Guide* incorrectly states that you can enter up to 30 alphanumeric characters in the Pickup Group Name field in the Call Pickup Group Configuration window. The guide should state that you can enter up to 100 characters in the Pickup Group Name field.

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" section on page 38.

The *Cisco Unified Communications Manager Features and Services Guide* does not state that the assistant console application supports Windows Vista.

Disregard the entire section, Assistant Console Dialog Options, in the *Cisco Unified Communications Manager Features and Services Guide*. Instead, use the information in the " Cisco Unified Communications Manager Assistant" section on page 38.

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.

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

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**.

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.

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( ).

- RSVP Reservation Teardown for Shared-Line Calls, page 95
- Destination Number in Remote Destination Configuration Window, page 95

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.

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 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).

Updates

This section provides information that has been updated since the release of the Cisco Unified Communications Manager Release 6.1(1a) documentation.

- Updated List of Fields Supported for Export by the Import/Export Tool, page 96
- Missing MIB Changes, page 97

Updated List of Fields Supported for Export by the Import/Export Tool

The *Cisco Unified Communications Manager Bulk Administration Guide* requires updates for these changes:

- In addition to the fields listed in the *Cisco Unified Communications Manager Bulk Administration Guide* 6.1(1) under System Data, the Import/Export tool also supports the **Server** field for export.
- The following fields listed in the *Cisco Unified Communications Manager Bulk Administration Guide* 6.1(1) under Call Routing Data are not supported for export by the Import/Export tool:
  - Route Group
  - Route List
  - Route Pattern
  - Line Group
  - Hunt List

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.

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 using the IVR during a call.

Warning Displays When Enabling SIP Stack Trace

In the Trace Configuration window in Cisco Unified Serviceability, one of the trace filter settings that are available for Cisco CallManager SDI represents Enable SIP Stack Trace. Because enabling this log can cause severe performance degradation, the following warning now displays when you click the Enable SIP Stack Trace check box: Enabling SIP Stack Trace can cause extreme performance degradation especially during high traffic hours.

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
```

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 Press any key to continue.

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:

- Enter **a** to reset the administrator password.

- Enter **s** to reset the security password.
- Enter **q** to quit.

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.

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.

Unclear Documentation on Called Party Name Presentation

The *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* provide 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.

Cisco Unified IP Phone User Guides

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 controlled by the phone do not get maintained in your EM profile.

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.

Extension Mobility Successful Authentication Cache

The Extension Mobility application maintains a cache of all logged on user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user gets validated with information from the cache. This means that, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords get recognized.

Software Conference Bridge Not Supported

The Configuring Secure Conference Resources chapter in the *Cisco Unified Communications Manager Security Guide* requires this addition: Due to the performance impact to Cisco Unified Communications Manager processing, secure conferencing does not get supported on software conference bridge.

Throttling on SIP UDP Ports

The SIP and Cisco Unified Communications Manager chapter in the *Cisco Unified Communications Manager System Guide* requires this update for SIP UDP port throttling.

SIP UDP port throttle thresholds help prevent Denial of Service (DOS) attacks from SIP trunks and SIP stations. When the incoming packet rate exceeds the configured threshold for a SIP station or SIP trunk UDP port, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

The SIP Service Parameters section of this chapter does not include the following 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 9 describes the configurable threshold values:

Table 9 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.

Deleting a Server

The *Cisco Unified Communications Manager Administration Guide* does not provide the error messages that display when you attempt to delete a server. For information on these error messages, see the "Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration" section on page 15.

Disregard the entire section, "Deleting a Server," in the System-Level Configuration Settings chapter in the *Cisco Unified Communications Manager System Guide*. Instead, consider the following information when you delete a server:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node. When you attempt to delete a node, Cisco Unified Communications Manager Administration displays the message that is described in the " Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration" section on page 15.
- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.

Do Not Disturb Feature Priority

On Cisco Unified IP Phones, the text message that indicates the Do Not Disturb (DND) feature is active takes priority over the text message that indicates the user has new voicemail messages, which allows the user to know when DND is active. However, the text message that indicates the Call Forward All feature is active has a higher priority than DND.

Security Icons and Encryption

This subsection of the "Restrictions" section in the Security Overview chapter in the *Cisco Unified Communications Manager Security Guide* requires this addition:

If a call from an encrypted phone over a SIP trunk gets transferred back to an encrypted phone in its own cluster, the call does not get encrypted, and the lock icon does not display even though the encrypted phones exist in the same secure cluster.

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 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*

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.
```

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.

Changes

This section contains changes that have occurred since the release of the Cisco Unified Communications Manager Release 6.1 documentation. These changes may not appear in the current documentation or the online help for the Cisco Unified Communications Manager application:

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.

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.

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.

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.

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.

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.

During an upgrade from Cisco Unified CallManager Release 4.x, the system automatically converts the **ac** application user to a superprovider user and disassociates the devices that were previously associated to the application user.

To enable device security for the Cisco Unified Communications Manager Attendant Console, configure an ACDeviceAuthenticationUser application user and associate the attendant phones with that user.

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 using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation <required for IOS - optional for other>" section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Printed in the USA on recycled paper containing 10% postconsumer waste.