



Release Notes for Cisco Unified Communications Manager Release 6.1(2)

Updated February 29, 2012

This document contains information included in the release notes for Cisco Unified Communications Manager Releases 6.1(1), 6.1(1a), and 6.1(1b) and new information for Cisco Unified Communications Manager Release 6.1(2). [Table 1](#) describes the additions and changes made for Release 6.1(2)

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the [“Upgrading to Cisco Unified Communications Manager 6.1\(2\)” section on page 3](#) for information about upgrading and the [“Important Notes” section on page 5](#) for information about issues that may affect your system.

To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL:

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



Note

Cisco recommends that you check [Cisco.com](http://www.cisco.com) for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the [“Before You Begin” section on page 3](#).

Contents

These release notes discuss the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading to Cisco Unified Communications Manager 6.1\(2\), page 3](#)
 - [Before You Begin, page 3](#)
 - [Upgrade Paths To Cisco Unified Communications Manager 6.1\(2\), page 3](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Upgrading from Unified CM 4.x and 5.x, page 3](#)
- [Cisco Recommendations, page 4](#)
- [Upgrading from Cisco Unified Communications Manager Release 6.0.\(1a\) or higher to Release 6.1\(2\) by Using the UCSInstall File, page 4](#)
- [Related Documentation, page 5](#)
- [Important Notes, page 5](#)
- [New and Changed Information in Cisco Unified Communications Manager 6.1\(2\), page 22](#)
- [Caveats, page 98](#)
 - [Table 7 Open Caveats as of April 21, 2008, page 101](#)
- [Documentation Updates, page 103](#)
- [Obtaining Documentation and Submitting a Service Request, page 103](#)

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 CM Release 6.1(2) on a Cisco Media Convergence Server (MCS) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS are compatible with Cisco Unified CM Release 6.1(2), refer to the Supported Servers for Cisco Unified Communications Manager Releases:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.



Note

Make sure that the matrix indicates that your server model supports Cisco Unified Communications Manager Release 6.1(3b).

Some servers that are listed in the compatibility matrix may require additional hardware support for Cisco Unified Communications Manager Release 6.1(2). 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.

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 to Cisco Unified Communications Manager 6.1(2)

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

- [Before You Begin, page 3](#)
- [Upgrade Paths To Cisco Unified Communications Manager 6.1\(2\), page 3](#)
- [Upgrading from Unified CM 4.x and 5.x, page 3](#)
- [Cisco Recommendations, page 4](#)
- [Upgrading from Cisco Unified Communications Manager Release 6.0.\(1a\) or higher to Release 6.1\(2\) by Using the UCSInstall File, page 4](#)

Before You Begin

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

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

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

Upgrade Paths To Cisco Unified Communications Manager 6.1(2)

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

**Caution**

Use the ISO files that are mentioned in the “[Upgrading from Cisco Unified Communications Manager Release 6.0.\(1a\) or higher to Release 6.1\(2\) by Using the UCSInstall File](#)” section on page 4 for upgrades from 6.x only.

Upgrading from Unified CM 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 that is for registered customers only](#) to obtain a media kit and license or to purchase the upgrade from Cisco Sales.

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

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.htm

Cisco Recommendations

Cisco offers the following recommendations.

Table 1 Cisco Recommendations

If you currently use:	Do this:
Unified CM Release 6.1(1), 6.1(1a), or 6.1(1b)	Upgrade to Unified CM 6.1(2)
A Unified CM Release 6.1(1), 6.1(1a), or 6.1(1b) Engineering Special	Contact TAC to obtain the fixes that are included in Release 6.1(1b)

Upgrading from Cisco Unified Communications Manager Release 6.0.(1a) or higher to Release 6.1(2) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_6.1.2.1000-13.sgn.iso, comprises two parts:

- UCSInstall_UCOS_6.1.2.1000-13.sgn.iso_part1of2
- UCSInstall_UCOS_6.1.2.1000-13.sgn.iso_part2of2

Procedure

-
- Step 1** From www.cisco.com, download the two UCSInstall files.
 - Step 2** Execute one of the following commands to reunite the two parts of the file.



Note Because the 6.1.2.1000-13 build is a nonbootable ISO, it proves useful only for upgrades. You cannot use it for new installations.

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

```
cat UCSInstall_UCOS_6.1.2.1000-13.sgn.iso_part1of2 UCSInstall_UCOS_6.1.2.1000-13.sgn.iso_part2of2 > UCSInstall_UCOS_6.1.2.1000-13.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_6.1.2.1000-13.sgn.iso_part1of2+UCSInstall_UCOS_6.1.2.1000-13.sgn.iso_part2of2 UCSInstall_UCOS_6.1.2.1000-13.sgn.iso

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

```
68e99f0b080298d65b4b82a8befbfe8b UCSInstall_UCOS_6.1.2.1000-13.sgn.iso
```

Software Download URLs

You can access the latest software upgrades for Cisco Unified Communications Manager at <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

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/vtgscal/>.

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(2). 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(2).

- [During GUI Login, Incorrect UserID Produces Incorrect Error Message, page 7](#)
- [Cisco CallManager Service Stops After Upgrade to Cisco Unified Communications Manager 6.X, page 7](#)
- [Important Information about Delete Transaction Using Custom File in BAT, page 7](#)

- [Cisco Unified Communications Manager Does Not Support Recovery of Administration or Security Passwords, page 7](#)
- [Deleting a Server and Adding a Deleted Server to a Cluster, page 8](#)
- [Clarification for Call Park Configuration, page 9](#)
- [Viewing Privileges for Roles in Cisco Unified CM Administration, page 9](#)
- [Basic Uninterruptible Power Supply \(UPS\) Integration, page 10](#)
- [CSCsq22385 Database Replication Setup Fails After You Add a New Subscriber to a Cluster, page 10](#)
- [Strict Version Checking, page 12](#)
- [Serviceability Not Always Accessible from OS Administration, page 13](#)
- [Voice Mailbox Mask Interacts with Diversion Header, page 13](#)
- [Installation Note for CTL Client 5.0 Plug-In, page 13](#)
- [Installation Note for Windows 2000 Users, page 14](#)
- [Cisco Unified IP Phones, page 61](#)
- [Using Call Pickup Groups with BLF Pickup, page 68](#)
- [Parallel Installations of Cisco Unified Communications Manager 6.1\(2\), page 71](#)
- [Parallel Upgrades from Unified CM Releases 5.x and 6.x to Unified CM Release 6.1\(2\), page 72](#)
- [Parallel Upgrades from Unified CM Release 4.x to Unified CM Release 6.1\(2\), page 72](#)
- [Installation Note, page 14](#)
- [Out of Service Nodes and Cisco License Manager, page 14](#)
- [Reset the Cluster After You Change the Security Password, page 14](#)
- [Best Practices for Assigning Roles to Serviceability Administrators, page 15](#)
- [For Serviceability, the Administrator That is Created During Installation Must Not Be Removed, page 15](#)
- [Clarification for Call Park Configuration, page 15](#)
- [Connecting to Third-Party Voice Messaging Systems, page 16](#)
- [Resetting Database Replication When Reverting To an Older Product Release, page 16](#)
- [User Account Control Pop-up Window Displays During Installation of RTMT, page 17](#)
- [CiscoTSP Limitations on Windows Vista Platform, page 17](#)
- [Time Required for Disk Mirroring, page 17](#)
- [Cisco Unified Mobility Supports Nine Locales, page 17](#)
- [Each Remote Destination Supports a Maximum of Two Active Calls, page 17](#)
- [Changes to Cisco Extension Mobility After Upgrade, page 18](#)
- [RTMT Requirement When Cisco Unified Communications Manager Is Upgraded, page 18](#)
- [Changes to Cisco Extension Mobility After Upgrade, page 18](#)
- [Serviceability Session Timeout Not Graceful, page 18](#)
- [Problem Configuring Mobility Identity for Nokia S60 Device in Cisco Unified Communications Manager Administration, page 18](#)
- [Updating the IP Address in the Server Configuration Window, page 19](#)

- [Deleting Then Adding Back a Server in Cisco Unified Communications Manager Administration](#), page 20
- [SIP Network/IP Address Field Required for SIP Fallback to SRST Gateway](#), page 21
- [Cisco Unified Reporting Application](#), page 21
- [CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value](#), page 21
- [CSCtx86215 Database Replication](#), page 21

During GUI Login, Incorrect UserID Produces Incorrect Error Message

If you use an incorrect userid when you log in to the Unified CM GUI, a database communication error message displays instead of the "Log on failed - Invalid User ID or Password" message.

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

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

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

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

Important Information about Delete Transaction Using Custom File in BAT

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

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

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

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

Deleting a Server and Adding a Deleted Server to a Cluster

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

**Tip**

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

Before you delete a server, consider the following information:

- Cisco Unified CM Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.
- Cisco recommends that you do not delete any node that has Cisco Unified CM running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified CM on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified CM Administration.
- If a configuration field in Cisco Unified CM Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.
- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or hostname for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.
- Changes to the server configuration do not take effect until you restart Cisco Unified CM. For information about restarting the Cisco CallManager service, refer to the serviceability documentation for Cisco Unified CM.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server.
- After you delete the node, access Cisco Unified Reporting to verify Cisco Unified CM removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

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

Procedure

-
- Step 1** In Cisco Unified CM Administration, add the server by choosing **System > Server**.
- Step 2** After you add the subsequent node to Cisco Unified CM Administration, perform an installation on the server by using the disk that Cisco provided in your software kit.



Tip For example, if you have a version 6.1(2) disk, perform a 6.1(2) installation on the node. If you have a disk with a compatible version of 5.X on it, for example, use the disk to install Cisco Unified CM on the subsequent node; during the installation, choose the **Upgrade During Install** option when the installation displays the options.

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

If the first node in the cluster runs Cisco Unified Communications Manager 6.1(2) version and a service release (or engineering special), you must choose the **Upgrade During Install** option when the installation displays the installation options; before you choose this option, ensure that you can access the service release (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, refer to installation documentation that supports your version of Cisco Unified CM.

- Step 3** After you install Cisco Unified CM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco Unified CM.
- Step 4** Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Clarification for Call Park Configuration

Consider the following information when you configure Call Park:

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

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

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

Viewing Privileges for Roles in Cisco Unified CM Administration

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

TAPS Name Change in Bulk Administration Tool

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

For More Information

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

Basic Uninterruptible Power Supply (UPS) Integration

When Cisco Unified Communications Manager 6.0(1a) runs on an MCS 7825H2 or MCS 7835H2, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported. Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, on MCS-7835H2, you can execute the **show ups** CLI command 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.

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

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

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

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

Other Symptoms

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

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

```
dbl_repl_cdr_define_lg_sub_8_ccm6_1_2_1000_13-2008_05_07_12_00_20.log

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

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

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

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

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

Workaround for a Single Node

Use the following workaround for this caveat.



Caution

Before you continue, identify the exact subscriber that is affected. To do that, look at the alert and confirm the node (IP) and the Node ID (hostname). In the preceding example alert, that information is node 10.1.1.1. App ID: Cisco AMC Service Cluster ID: Node ID: xxx

Step 1

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

Step 2

From the platform CLI on the SUBSCRIBER, enter the following command:

```
utils dbreplication stop.
```



Caution

This process can take 5 minutes or more to complete.

Wait for it to finish before you continue.

Step 3

From the platform CLI on the SUBSCRIBER, enter the following command:

```
utils dbreplication dropadmindb
```

Step 4

From the platform CLI on the PUBLISHER, enter the following command.

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

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

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

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

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

Workaround for Multiple Nodes

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

Verification

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

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

Strict Version Checking

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



Note

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

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

Table 2 **Restore Examples**

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

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

Serviceability Not Always Accessible from OS Administration

In some scenarios, you cannot access the Cisco Unified Serviceability from Cisco Unified OS Administration. The page displays a “Loading, please wait” message indefinitely.

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

Voice Mailbox Mask Interacts with Diversion Header

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

Installation Note for CTL Client 5.0 Plug-In

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

Procedure

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

<http://support.microsoft.com/kb/290301>
 - Step 2** Install the utility on your PC.
 - Step 3** Run the utility.
 - Step 4** Find eToken rte3.0 in the list of programs and remove it.
 - Step 5** Proceed with CTL Client installation.
-

Installation Note for Windows 2000 Users

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

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

**Note**

Windows 2000 comes with Windows Installer 2.0.

Windows Installer 3.0 requires validation. Follow the instructions to have your PC validated; then, install Windows Installer 3.0; reboot your machine, if necessary, and proceed with CTL Client installation.

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 of 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 CSCs157629 and CSCs157655.

`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 Destinations 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 143](#), 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*.

CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value

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

CSCtx86215 Database Replication

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

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

New and Changed Information in Cisco Unified Communications Manager 6.1(2)

The following section describes new features and changes that are pertinent to Cisco Unified Communications Manager, Release 6.1(2) or later. The sections may include configuration tips for the administrator, information about users, and information about where to find more information.

- [Improved Access to Personal Address Book, page 22](#)
- [Cisco VGD-1T3 Voice Gateway Support in Cisco Unified Communications Manager Administration, page 23](#)
- [Upgrading to Unified CM Release 6.1\(2\) from Supported Cisco Unified CallManager 4.x Releases by Using a Configuration File, page 24](#)
- [Disaster Recovery Manual Backup Window, page 24](#)
- [Cisco Unified Communications Operating System CLI Commands, page 25](#)
- [Installation, Upgrade, Migration, and Disaster Recovery, page 40](#)
- [Cisco Unified Communications Operating System Administration, page 41](#)
- [Cisco Unified Communications Manager Administration, page 42](#)
- [Cisco Unified Communications Manager Features and Applications, page 46](#)
- [Cisco Unified Communications Manager Bulk Administration Tool, page 55](#)
- [Cisco Unified Serviceability, page 56](#)
- [CDR Analysis and Reporting Tool/Call Detail Record \(CAR/CDR\), page 59](#)
- [Cisco Unified Communications Manager User Options, page 60](#)
- [Cisco Unified IP Phones, page 61](#)
- [Using Call Pickup Groups with BLF Pickup, page 68](#)
- [Parallel Installations of Cisco Unified Communications Manager 6.1\(2\), page 71](#)
- [Parallel Upgrades from Unified CM Releases 5.x and 6.x to Unified CM Release 6.1\(2\), page 72](#)
- [Parallel Upgrades from Unified CM Release 4.x to Unified CM Release 6.1\(2\), page 72](#)
- [Enhancements for Cisco Unified CM User Options, page 73](#)
- [Enhancements for Data Migration Assistant, page 73](#)
- [Enhancements for the Disaster Recovery System, page 74](#)
- [Changing the Hostname of Cisco Unified Communications Manager Servers, page 74](#)
- [Enhancements for Cisco Unified Serviceability, page 75](#)
- [Enhancements for Cisco Unified Reporting, page 77](#)
- [Cisco Unified Reporting, page 78](#)
- [Cisco and Third-Party APIs, page 79](#)

Improved Access to Personal Address Book

Administrators can now set up a service URL that allows users to get fast access to their Personal Address Book (PAB) as a service without having to authenticate each time:

The administrator modifies a phone button template to associate a service URL and then assigns the phone button template to the user's phone.

In Cisco Unified CM User Options, the user assigns the service URL to an existing line button on the phone. The user can then press the line button to access the PAB without having to authenticate.

Cisco Unified CallManager Administration Configuration Tips

Use the following tips to configure fast access to PAB in Cisco Unified Communications Manager Administration:

- Configure PAB as an IP phone service.
- Modify a phone button template to associate a service URL with a line button

GUI Changes

The following fields on the IP Phone Services Configuration parameters support creation of the PAB phone service.

- **Service Name** and **ASCII Service Name**—Enter a name to identify the service.
- **Service URL**—Enter the URL to access the PAB.

User Tips

In Cisco Unified CM User Options, the user assigns the service URL to an existing line button on the phone. The user can then press the line button to access the PAB without having to authenticate.

Before the user can assign a line button for PAB, the system administrator must configure the phone to display services.

For More Information

- IP Phone Services Configuration, *Cisco Unified Communications Manager Administration Guide*
- Phone Button Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Guidelines for Customizing Phone Button Templates, *Cisco Unified Communications Manager System Guide*
- Cisco Unified IP Phone Guides

Cisco VGD-1T3 Voice Gateway Support in Cisco Unified Communications Manager Administration

After the Cisco VGD-1T3 Voice Gateway releases, you can configure the gateway in Cisco Unified Communications Manager Administration 6.1(2).

The Cisco VGD-1T3 is a high density voice gateway with up to 1 Channelized T3 [CT3] of voice over IP [VoIP] capacity with support for Cisco Unified Communications Manager and Cisco Voice Portal (CVP) applications with Media Gateway Control Protocol (MGCP). The VGD-1T3 Voice Gateway offers unparalleled capacity in only two rack units (2RUs) and provides best-of-class voice and fax services. Feature support includes:

- Cisco Unified Communications Manager MGCP support
- SIP / H.323 support
- Cisco Unified Communications Manager MTP (Media Termination Point), transcoder support, RSVP agent

- Support for three VGD-1T3 system per Cisco Unified Communications Manager server
- Future support for Cisco Unified Communications Manager conference bridge

To configure this gateway in Cisco Unified Communications Manager Administration, choose Device > Gateway. Click **Add New** and choose **Cisco VGD-1T3** from the Gateway Type drop-down list box. After you click **Next**, the Gateway Configuration window displays.

**Tip**

No new configuration settings were added to Cisco Unified Communications Manager Administration to support this gateway. For additional information on how to configure gateways in Cisco Unified Communications Manager Administration, refer to the "Gateway Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide, Release 6.1(1)*.

Upgrading to Unified CM Release 6.1(2) from Supported Cisco Unified CallManager 4.x Releases by Using a Configuration File

To use the configuration file that Data Migration Assistant generated to prepopulate fields during an upgrade of the first node to Cisco Unified Communications Manager 6.1(2) from supported releases of Cisco Unified CallManager 4.x, copy the platformConfig.xml file to a USB key before you boot the server with the Cisco Unified Communications Manager 6.1(2) DVD.

If you use the platformConfig.xml file during the upgrade, some windows do not display, and some fields that are described in the *Upgrading to Cisco Unified Communications Manager Release 6.1(2) from Cisco Unified Communications Manager 4.x Releases* document get prepopulated.

You can change any of the prepopulated fields, if necessary.

GUI Changes

The Cisco Unified Communications Manager system prepopulates several fields during the upgrade process based on the information that the platformConfig.xml file contains.

Installation/Upgrade (Migration) Considerations

If you use the platformConfig.xml file during the upgrade, some windows do not display and some fields get prepopulated that are described in the *Upgrading to Cisco Unified Communications Manager Release 6.1(2) from Cisco Unified Communications Manager 4.x Releases* document.

You must insert the USB key into the server before you boot the first node with the Cisco Unified Communications Manager 6.1(2) DVD.

For More Information

For more information, see the *Upgrading to Cisco Unified Communications Manager Release 6.1(2) from Cisco Unified Communications Manager 4.x Releases*.

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 *outfile*

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 *outfile*.
- **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 *outfile*

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 *outfile*.
- **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.
- **sftplot** 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
```

```
active log { filename filename | directory | sort }
```

```
common { filename filename | directory | sort }
```

```
inactive log { 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 setreptimeout

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

Command Syntax

utils dbreplication setreptimeout *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 command the **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 40](#)
- [Where to Find More Information, page 41](#)

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:

- [Overview, page 42](#)
- [Browser Requirements, page 42](#)
- [NIC Teaming Support, page 42](#)
- [Where to Find More Information, page 41](#)

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.

NIC Teaming Support

Server platforms with dual Ethernet network interface cards (NICs) can support NIC teaming for network fault tolerance with Cisco Unified Communications Manager. Cisco began support of NIC teaming on HP servers in the 5.0(1) release and began support on IBM servers in the 6.1(2) release. This feature allows a server to be connected to the Ethernet via two NICs and, hence, two cables. NIC teaming prevents network downtime by transferring the workload from the failed port to the working port. NIC teaming cannot be used for load balancing or increasing the interface speed.

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:

- [When to Log In To the Console, page 43](#)
- [Browser Requirements for Cisco Unified Communications Manager Administration, page 43](#)
- [Service Parameter and Enterprise Parameter Changes, page 43](#)
- [Menu Changes, page 45](#)
- [Where to Find More Information, page 45](#)

When to Log In To the Console

Cisco does not recommend logging onto the console during busy hours since it will consume additional CPU resources. This can lead to Code Yellow or Code Red alarms depending on the tasks being performed and the CPU utilized to perform those tasks. It is recommended that console usage (remote or local) should be used to do maintenance or upgrades during maintenance windows.

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 43.)
- **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 Users**—Primary User Device (new field); works in conjunction with Enable Mobility check box.
- **Bulk Administration > 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 Administration > 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:

- [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., page 145](#)
- [Intercom for Cisco Extension Mobility, page 48](#)
- [Join Across Lines, page 49](#)
- [Licensing for Cisco Unified Mobility, page 50](#)
- [Single Button Barge, page 51](#)
- [SIP Trunk Identification, page 52](#)
- [Thai Language Support, page 53](#)
- [Turkish Language Support, page 53](#)
- [Phone Button Template, Line, and Security Enhancements for the Nokia S60 Device, page 53](#)

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.

Serviceability 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 55](#).

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-configurable 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 61](#).

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 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 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 > 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 55](#).

AXL and CTI Considerations

For information on how join across lines works with AXL, see the [“Cisco and Third-Party APIs” section on page 79](#).

User Tips

For information on phone support for join across lines, see the [“Cisco Unified IP Phones” section on page 61](#).

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 55.

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 79.

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 55.

AXL and CTI Considerations

For information on how join across lines works with AXL, see the [“Cisco and Third-Party APIs”](#) section on page 79.

User Tips

For information on phone support for single button barge, see the [“Cisco Unified IP Phones”](#) section on page 61.

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 79.

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 18

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:

- [New Preconfigured Alerts in Cisco Unified Serviceability, page 56](#)
- [New Highlight Capability on RTMT Graphs and Charts, page 56](#)
- [Consistent RTMT Severity and Syslog Severity, page 56](#)
- [Collecting Installation Logs, page 57](#)
- [Database Summary Includes Database Replication Information, page 57](#)
- [New Preconfigured Alerts in Cisco Unified Serviceability, page 57](#)
- [RTMT Critical Services, page 57](#)
- [Adding RTMT Performance Counters in Bulk, page 58](#)
- [RTMT Trace and Log Central Disk IO and CPU Throttling, page 58](#)
- [Trace Compression Support, page 58](#)

New Preconfigured Alerts in Cisco Unified Serviceability

The following list shows preconfigured alerts that are now available:

- **DBChangeNotifyFailure:** This alert occurs when the Cisco Database Notification Service is experiencing problems and could be halted. This condition indicates that Change Notification Requests that are queued in the database are “stuck” and system changes are not taking effect. If you use the default alert properties, the alert gets triggered when the DBChangeNotify queue delay is over 2 minutes; one alert gets sent every 30 minutes.
- **NumberofRegisteredDevicesExceeded:** This alert flags a critical overload condition that may impact phone registration. If you use the default alert properties, an alert gets sent for every NumDevRegExceededalarm.

New Highlight Capability on RTMT Graphs and Charts

The RTMT adds a new highlight capability to help distinguish hosts and counters when multiple nodes or counters display on color-coded graphs. To implement this feature,

- Right-click in a plot area to highlight the nearest data series or point for the following charts and graphs: System Summary, CPU and Memory, Disk Usage, and Performance Log Viewer.
- Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Highlight** to highlight the data series for that counter.
- Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Change Color** to select a different color for the counter.

A highlighted item returns to its original appearance when you select another item to highlight.

Consistent RTMT Severity and Syslog Severity

Severity levels for Syslog entries now match the severity level for all RTMT alerts. If an RTMT issues a critical alert, the corresponding Syslog entry also specifies critical.

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 103.

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](#), page 59
- [Automatically Generated Reports](#), page 59
- [Automatic E-Mail Alerts](#), page 59
- [Tbl_pregenmail_option Table Data](#), page 59
- [Calculation of the Utilization of H.323 Gateways](#), page 60
- [CDR Search Reports Display Time in Two Ways](#), page 60
- [CAR Scheduler Now a Network Service](#), page 60

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 hhmss, 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 61](#)
- [Cisco Unified IP Phone 7965G and 7945G, page 62](#)
- [Cisco Unified IP Phone 7962G and 7942G, page 62](#)
- [Cisco Unified IP Conference Station 7937G, page 63](#)
- [Connection Monitor, page 63](#)
- [Intercom with Cisco Extension Mobility, page 64](#)
- [Single Button Barge \(SCCP\), page 64](#)
- [Join Across Lines \(SCCP\), page 65](#)
- [Cisco Unified IP Phone Support for Cisco Unified Communications Manager 6.1 Features, page 65](#)
- [Busy Lamp Field, page 66](#)
- [Cisco Unified IP Phone Expansion Modules, page 67](#)
- [Call Park Reversion \(Inconsistent Messages\), page 67](#)

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

Table 3 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 65
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 64

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

Cisco Unified Communications Manager 6.1 Feature	Cisco Unified IP Phone Support	For more information, see
Single Button Barge	SCCP only: 7975G 7971G-GE 7970G 7961G-GE 7941G-GE 7962G 7942G 7965G 7945G	Single Button Barge (SCCP), page 64

Busy Lamp Field

The existing Busy Lamp Field (BLF) feature allows the end user to monitor the state of the phone line of another user. The detectable line states include busy, idle, or DND. The line that BLF monitors comprise a speed-dial button, call log, or directory listing on the phone of the local user.

Cisco Unified Communication Manager 6.1(2) introduces BLF Pickup, which provides the following enhancements to the existing BLF feature:

BLF Alerting Line State

This enhancement adds alerting (ringing) to the detectable line states. BLF Pickup notifies the user when a monitored speed-dial line is ringing by providing an animated icon, amber flashing line button, and optional audible alert. The administrator can turn the audible alert on or off.

BLF Pickup Action

If a line is in the BLF alerting state, the local user can press the associated speed-dial button (BLF Pickup button) to pick up the call. The phone picks up the call on the next available line if the user does not first specify a line. If auto-pickup is enabled for the line, the call connects automatically; otherwise, the call rings on the local phone, and the user must manually answer it.



Note

Pressing the BLF Pickup button at a time when no BLF alerting indicators are present results in the phone speed dialing the associated directory number.

Unlike the existing BLF feature, you cannot configure BLF Pickup for a call log or directory listing; BLF Pickup works on a speed-dial line button only.

The following phones that are running SCCP support these BLF enhancements:

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

- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G

Where to Find More Information

For more information, see the [“Using Call Pickup Groups with BLF Pickup”](#) section on page 68.

Cisco Unified IP Phone Expansion Modules

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



Note

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

Where to Find More Information

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

Call Park Reversion (Inconsistent Messages)

Depending on which protocol a Cisco Unified IP Phone uses, users will see different status messages during a Call Park Reversion scenario (the time that a call remains parked). Cisco Unified IP Phones with SCCP will display the following message on the phone screen:

From XXXX

Cisco Unified IP Phones with SIP will display the following message on the phone screen:

Call Park Reversion (XXXXXXXXXX)



Note

To see a similar message on the SCCP phone screen, set the Caller ID Display Priority Enabled service parameter to **False**.

Call Park Reversion uses the following service parameters:

- Call Park Display Timer
- Caller ID Display Priority Enabled (used for SCCP phones only)
- Call Park Reversion Timer

For more information, see the “Call Park and Directed Call Park” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Using Call Pickup Groups with BLF Pickup

The Busy Lamp Field (BLF) Pickup feature adds call pickup capability to BLF SpeedDial buttons. When enabled, this feature alerts a user when a BLF SpeedDial destination gets an incoming call so that the user can pick up the call. Call pickup groups control which phones a user can monitor and access. A call pickup group can now include a hunt pilot to support line group pickup.

The busy lamp field indicates the line state at the remote device. An animated icon, LED appearance, and optional tone indicate BLF alerting. You can enable audible alerts at the system and device level.

An alerting call state makes the BLF Pickup button function available. When the user presses the BLF Pickup button, the phone picks up the call.

- If the monitoring device has multiple lines, the system uses the primary line as the pickup line or the next available line if the primary line is not available.
- If the monitored destination is receiving multiple calls, the first call or the higher priority MLPP call gets picked up; any remaining calls continue to trigger the alerting status on the BLF Pickup button.
- If the user at a monitored destination answers the call before call pickup, the BLF Pickup button displays a busy status.

After call pickup, the BLF Pickup button status reverts to the current status for the monitored destination: idle, busy, or DND (when enabled with the “BLF Status Depicts DND” service parameter).

As administrator, you must modify the standard line button template to include the BLF SD option for users to invoke the BLF pickup feature. See “Configuring a Customized Phone Button Template for BLF SpeedDial Buttons” in the Presence chapter for more information.

The following phone models, which are equipped with BLF line buttons support the BLF pickup feature: Cisco Unified IP Phone 7931, Cisco Unified IP Phone 7941, Cisco Unified IP Phone 7961, Cisco Unified IP Phone 7970, and Cisco Unified IP Phone 7971. The Cisco Unified IP Phone Expansion Module 7914 supports this feature when it is connected to one of these phone models.

Adding Call Pickup to a BLF SpeedDial

Using a template that supports BLF SD, configure the BLF SpeedDial and enable call pickup for that destination in Cisco Unified Communications Manager Administration. See “Configuring BLF/SpeedDial buttons” for how to configure BLF Speed Dials.

You must also assign a subscriber calling search space to the monitoring device or the user will not receive BLF notifications. See “Configuring and Applying the SUBSCRIBE Calling Search Space” for more information.

Busy Lamp Field/Speed Dial Button Settings					
	Destination	Directory Number	Label	Label ASCII	CALL PICKUP
1		8001 in PT_BLF	BLF Pickup 8001	BLF Pickup 8001	<input checked="" type="checkbox"/>
2		6007	Speed Dial 6007	Speed Dial 6007	<input type="checkbox"/>

See Cisco Unified CallManager Administration Configuration Tips for more information about configuring call pickup groups, calling search spaces, and hunt pilots to support the BLF pickup feature.

Cisco Unified CallManager Administration Configuration Tips



Note

Cisco Unified Communications Manager Release 6.1(2) supports the BLF Pickup button for SCCP devices only.

Use the following tips to configure BLF pickup in Cisco Unified Communications Manager Administration:

- The BLF Pickup button can pick up SCCP or SIP calls.
- You can configure BLF SpeedDial button templates for a phone or user device profile.
- You can configure any destination within a cluster for the BLF pickup feature on supported phones.
- If you configure a BLF Speed Dial destination outside the cluster, the system does not send alerts or allow call pickup.
- The associated call pickup group of the call pickup group for the monitoring user must contain the pickup group for the monitored destination, or call pickup will fail.
- If you configure a BLF speed dial but do not associate the pickup group to the DN that is used for call pickup, the phone receives BLF call alerts, but the user receives a tone and cannot pick up the call.
- At installation, the BLF pickup audible alert settings default to Disable. You cannot configure audible alert settings on phones that do not support this feature. Changing the audible alert settings on a device requires a reset of the device.
- To implement BLF pickup for a line group, enter **CSCsb42763** in the enterprise parameter “Cisco Support Use 1” and add the hunt pilot number to a call pickup group.
- To monitor a destination in a hunt list, configure both the hunt pilot and member DNs in the same call pickup group. Users can then pick up incoming calls whether the alerting call is from the hunt list or a directed call to the destination. If the incoming call is from a hunt list, but the hunt pilot is not in an associated call pickup group, the Call Pickup button will pick up only calls that are directed to the hunt list member (not the hunt pilot).
- When the Auto Call Pickup Enabled service parameter specifies True, the user presses the BLF Pickup button to connect the call.
- When the Auto Pickup Enabled service parameter specifies False, the phone rings after the user presses the BLF Pickup button. The user then goes off hook or presses the Answer softkey to connect the call. If the user does not take the call or a line is not available, the call gets restored to its original destination, and the BLF Pickup button shows alerting status. If the alerting call is to a hunt pilot, the original call gets restored to the hunt list as a new call, and the hunt list restarts the hunt.
- BLF pickup stays disabled when DND Call Reject is enabled for the monitored or monitoring device.
- BLF alerting occurs if DND No Ring is enabled for the monitored device. If DND No Ring is enabled for the monitoring device, the device presents non-audible alerts and call pickup is allowed.
- The Call Pickup No Answer Timer and the Call Pickup Locating Timer service parameters apply to BLF pickup.

GUI Changes

The following Phone Configuration parameters control BLF pickup settings.

- **Call Pickup:** This check box in the Busy Lamp Field Speeddial Configuration window enables Call Pickup for a BLF SpeedDial destination.

- **BLF Audible Alert Setting (Phone Idle):** This parameter controls the audio alert for BLF pickup when the phone is idle (not in use). When the setting is Off, no ring tone is played. When the setting is On, the call waiting tone is played once. When the setting is Default, the value is taken from the BLF Pickup Audio Alert Setting of Idle Station service parameter.
- **BLF Audible Alert Setting (Phone Busy):** This parameter controls the audio alert for BLF pickup when the phone is busy. When the setting is Off, no ring tone is played. When the setting is On, the call waiting tone is played once. When the setting is Default, the value is taken from the BLF Pickup Audio Alert Setting of Idle Station service parameter.

Service Parameter and Enterprise Parameter Changes

The following service parameters control BLF pickup audible alerts for your system.

- **BLF Pickup Audio Alert Setting of Idle Station:** This required service parameter controls the audio alert for BLF pickup on a Cisco Unified Communications Manager system when the phone is idle (not in use). This setting becomes the system default. Valid values follow:
Disable -- No ring.
Play Tone -- Ring once.
Default species Disable.
- **BLF Pickup Audio Alert Setting of Busy Station** This service parameter controls the audio alert for BLF pickup on a Cisco Unified Communications Manager system when the phone is busy (in use). This setting becomes the system default. Valid values follow:
Disable -- No ring.
Play Tone -- Beep only.
Default specifies Disable.

Installation/Upgrade (Migration) Considerations

BLF Pickup, a system feature, comes standard with Cisco Unified Communications Manager software. After you install Cisco Unified Communications Manager, you must configure BLF pickup settings in Cisco Unified Communications Manager Administration to enable the feature.

BAT Considerations

BAT supports exports and import of this feature as part of the export/import phones transaction.

BAT administrators can configure BLF pickup in the Busy Lamp Field Speeddial Configuration window. BAT administrators can set BLF pickup audible alerts for a device in the Phone Template Configuration window, through the Update phones functionality in BAT, or through the BAT.xlt (CSV file) and create file format options at the BAT GUI.

Security Considerations

To prevent unauthorized monitoring/pickup of user DNs, only administrators can configure BLF Speed Dials and enable call pickup. Administrators must ensure that the watcher is authorized to monitor a destination that is configured as a BLF/SpeedDial button.

CTI Considerations

The AXL add/update/get phone API supports the optional tag 'BLFSdOptionBitMask' (blfSpeedDial.BlfSdOptionBitmask) under the parent tag 'busyLampField.' The default specifies 0.

The AXL add/update/get phone API supports the optional tags 'ringSettingIdleBLFAudibleAlert' (Device.tkBLFAudibleAlerting_Idle) and 'ringSettingBusyBLFAudibleAlert' (Device.tkBLFAudibleAlerting_Busy) under the parent tag 'busyLampField.' The default specifies 2.

User Tips

The BLF Pickup line button identifies the BLF pickup feature on your phone.

- To initiate an outgoing Speeddial, press the BLF Pickup button when the BLF status is idle (or busy). If an alert comes in while you are pressing BLF Pickup, the outgoing call continues, and the alerting call does not get picked up.
- To initiate a call pickup, press the BLF Pickup button when the BLF status is alerting.

This feature adds a flashing “alerting” status icon (see example following) to the existing BLF status icons: busy, idle, and DND (when configured with the BLF Status Depicts DND service parameter).



Phone users can enable or disable all audible phone alerts, including BLF pickup, with the DND softkey at the phone or the DND setting (when available) in the User Option Device window.

For More Information

- Configuring BLF/SpeedDial Buttons, *Cisco Unified Communications Manager Features and Services Guide*
- Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, *Cisco Unified Communications Manager Features and Services Guide*
- Phone Button Templates, *Cisco Unified Communications Manager System Guide*
- Guidelines for Customizing Phone Button Templates, *Cisco Unified Communications Manager System Guide*
- Programmable Line Keys, *Cisco Unified Communications Manager System Guide*
- Phone Button Template Configuration, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Cisco Unified IP Phone 7914 Expansion Module Phone Button Template, *Cisco Unified Communications Manager Administration Guide*
- Call Pickup Group, *Cisco Unified Communications Manager Features and Services Guide*
- Call Pickup Group, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
- Phone Features, *Cisco Unified Communications Manager System Guide*
- Phone Configuration Checklist, *Cisco Unified Communications Manager System Guide*
- Hunt Pilot Configuration, *Cisco Unified Communications Manager Administration Guide*
- Configuring and Applying the SUBSCRIBE Calling Search Space, *Cisco Unified Communications Manager Features and Services Guide*

Parallel Installations of Cisco Unified Communications Manager 6.1(2)

For Cisco Unified Communications Manager 6.1(2), administrators can begin the installation of the primary node and subsequent nodes at the same time. When the installation program prompts the administrator to designate the server as a primary node or subsequent node, administrators must stop installing Cisco Unified Communications Manager on the subsequent nodes until the installation completes on the primary node and the administrator configures the subsequent node(s) on the primary

node. Administrators can then continue the installation on the subsequent nodes. For optimal performance, administrators should choose the **Skip** option rather than the **Proceed** option in the Platform Administration Wizard.

Parallel Upgrades from Unified CM Releases 5.x and 6.x to Unified CM Release 6.1(2)

When you upgrade a cluster running a supported version of Cisco Unified Communications Manager 5.x or 6.x to Cisco Unified Communications Manager 6.1(2), begin upgrading the first node first. You can begin upgrading subsequent nodes in parallel after the first node has reached a specified point in the upgrade.

During the upgrade of the first node, view the installation log, `install_log_<date+time>.log`, using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or the command line interface (CLI). You can begin the upgrade of the subsequent nodes once the following information displays in the log.

PRODUCT_TARGET is <product target id>

PRODUCT_NAME is <product name>

PRODUCT_VERSION is <product version to which you are upgrading, such as 6.1(2)>



Caution

If you want to upgrade the subsequent nodes in parallel with the first node, do not choose the Reboot to upgraded partition on either first node or subsequent nodes while configuring the upgrade options. If selected, the first node may complete its upgrade and reboot while the subsequent nodes are upgrading, causing the upgrade of the subsequent nodes to fail.

Parallel Upgrades from Unified CM Release 4.x to Unified CM Release 6.1(2)

You can begin the installation of the primary node and subsequent nodes at the same time. When the installation program prompts you to designate the server as a primary node or subsequent node, you must stop installing Cisco Unified Communications Manager on the subsequent nodes until the installation completes on the primary node and you configure the subsequent node(s) on the primary node. After you have configured the subsequent nodes on the primary node, you can continue the installation on the subsequent nodes. For optimal performance, you should choose the Skip option rather than the Proceed option in the Platform Administration Wizard. For more information, refer to the *Upgrading to Cisco Unified Communications Manager Release 6.1(2) from Cisco Unified Communications Manager 4.x Releases* document.

Enhancements for Cisco Unified CM User Options

Description

In Cisco Unified Communications Manager 6.1(2), you can control whether the end user can view the manager name and user ID in the Directory Find/List window in Cisco Unified CM User Options.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

The Show Manager in Directory and Show User ID in Directory enterprise parameters in Cisco Unified Communications Manager Administration allow you to control whether the end user can view the manager name and User ID in the Directory Find/List window in Cisco Unified CM User Options. For information on these parameters, see the [“Service Parameter and Enterprise Parameter Changes” section on page 73](#).

Service Parameter and Enterprise Parameter Changes

To access the following enterprise parameters in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

- **Show Manager Name in Directory**—This parameter determines whether to display the Manager Name in the Directory Find/List window in Cisco Unified CM User Options. This required field includes a default of True, which means that the Manager Name displays. The change takes effect the next time that the user logs in to Cisco Unified CM User Options.
- **Show User ID Name in Directory**—This parameter determines whether to display the User ID in the Directory Find/List window in Cisco Unified CM User Options. This required field includes a default of True, which means that the User ID displays. The change takes effect the next time that the user logs in to the Cisco Unified CM User Options.

Installation/Upgrade (Migration) Considerations

After you install or upgrade to Cisco Unified Communications Manager 6.1(2), you can configure this functionality.

User Tips

After you configure the enterprise parameters, the change takes effect the next time that the end user logs in to Cisco Unified CM User Options.

For More Information

For more information on the Cisco Unified CM User Options, refer to the Cisco Unified IP Phone user documentation that supports your phone model.

Enhancements for Data Migration Assistant

The Data Migration Assistant 6.1(2) generates a configuration file (platformConfig.xml) that can assist you in performing an upgrade of the first node to Cisco Unified Communications Manager 6.1(2) from supported releases of Cisco Unified CallManager 4.x. The configuration file prepopulates several fields during the upgrade, including domain name, IP address, primary DNS, secondary DNS, and NTP server.

To use the configuration file, copy the platformConfig.xml file to a USB key, and place the USB key into the Cisco Unified Communications Manager first node before you boot the server with the Cisco Unified Communications Manager 6.1(2) DVD.

If you choose to store the DMA tar file on a network directory or local directory, DMA stores the platformConfig.xml in the same directory. If you choose to store the DMA tar file on a tape drive, DMA stores the platformConfig.xml in D:/DMA.

**Note**

Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys will have a W95 FAT32 format.

Installation/Upgrade (Migration) Considerations

To use the configuration file that Data Migration Assistant generates to prepopulate fields during and upgrade to Cisco Unified Communications Manager 6.1(2) from supported releases of Cisco Unified CallManager 4.x, copy the platformConfig.xml file to a USB key before you boot the server with the Cisco Unified Communications Manager 6.1(2) DVD.

For More Information

Refer to the *Data Migration Assistant User Guide*.

Enhancements for the Disaster Recovery System

In this release, the Disaster Recovery System automatically backs up the backup device that you have configured in the Select Backup Device area of the Backup Device List window and the scheduled backups that you configured on the Schedule List window when you back up your system. When you perform a restore, the system restores the backup device and schedule, so you do not have to reconfigure those settings.

The Disaster Recovery System also provides status of the current restore procedure on the Restore Status window.

GUI Changes

The Restore Status window in the Disaster Recovery System contains a new Status column. This column shows the status of the restoration in progress, including the percentage of completion of the restore procedure. To access the Restore Status window, choose **Restore > Status**.

For More Information

For more information on the Disaster Recovery System, refer to the *Disaster Recovery System Administration Guide*.

Changing the Hostname of Cisco Unified Communications Manager Servers

Starting with this release, you can change the hostname of the first node or any subsequent nodes in the Cisco Unified Communications Manager cluster. You can only change the hostname of the first node from a subsequent node. The Cisco Unified Communications Operating System Administration user interface populates the hostname field on the Ethernet Configuration window and the Publisher Configuration window with the existing values. You can change the IP address or hostname of servers using the set network cluster publisher ip or set network cluster publisher hostname CLI commands.

**Caution**

Resetting the hostname will cause your system to reboot, and you may lose connectivity with the first node and the network. Before attempting to change the hostname of a Cisco Unified Communications Manager server, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 6.1(2)*.

Cisco Unified Communications Manager Administration Configuration Tips

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

GUI Changes

The Ethernet Configuration window and the Publisher Configuration window in the Cisco Unified Operating System Administration contain a new Hostname field. The fields get populated with the existing values.

For More Information

For more information, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 6.1(2)*.

Enhancements for Cisco Unified Serviceability

This section contains these subsections:

- [New Preconfigured Alerts in Cisco Unified Serviceability, page 75](#)
- [New Highlight Capability on RTMT Graphs and Charts, page 75](#)
- [Consistent RTMT Severity and Syslog Severity, page 76](#)
- [CAR - Configuring Individual and Department Bills Reports, page 76](#)

New Preconfigured Alerts in Cisco Unified Serviceability

The following list shows preconfigured alerts that are now available:

- **DBChangeNotifyFailure:** This alert occurs when the Cisco Database Notification Service is experiencing problems and could be halted. This condition indicates that Change Notification Requests queued in the database are “stuck” and system changes are not taking effect. If you use the default alert properties, the alert gets triggered when the DBChangeNotify queue delay is over 2 minutes; one alert gets sent every 30 minutes.
- **NumberofRegisteredDevicesExceeded:** This alert flags a critical overload condition that may impact phone registration. If you use the default alert properties, an alert gets sent for every NumDevRegExceededalarm.

New Highlight Capability on RTMT Graphs and Charts

The RTMT adds a new highlight capability to help distinguish hosts and counters when multiple nodes or counters display on color-coded graphs. To implement this feature

- Right-click in a plot area to highlight the nearest data series or point for the following charts and graphs: System Summary, CPU and Memory, Disk Usage, and Performance Log Viewer.

- Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Highlight** to highlight the data series for that counter.
- Right-click on any color code in the table below the chart in the Performance Log Viewer and choose **Change Color** to select a different color for the counter.

A highlighted item returns to its original appearance when you select another item to highlight.

Consistent RTMT Severity and Syslog Severity

Severity levels for Syslog entries now match the severity level for all RTMT alerts. If an RTMT issues a critical alert, the corresponding Syslog entry also specifies critical.

CAR - Configuring Individual and Department Bills Reports

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

Procedure for Adding Owner User ID to Individual Bills

To add an owner user ID, perform the following tasks:

- In Cisco Unified Communications Manager Administration, choose **Device > Phone > Add a New Phone > Phone Configuration**.
- Add the information for the device and the user.

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

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

To add an owner user ID and manager ID, perform the following tasks:

- In Cisco Unified Communications Manager Administration, choose **Device > Phone > Add a New Phone > Phone Configuration**.
- Add the information for the device and the user.

and

- In Cisco Unified Communications Manager Administration, choose **User Management > End User > Add**.
- Add the Manager User ID information to the end user information.

For both individual bills and department bills, if the extension mobility feature is

- Enabled on the device and the user logs into the phone and places a call, the User ID that gets recorded in the CDRs is the logged in User ID.
- Not enabled on the device, the User ID that gets recorded in the CDRs is the "Owner User ID" that is configured for the device.
- If neither the User ID nor the Owner User ID is configured (that is, extension mobility is not enabled, and the Owner User ID is not configured), the User ID field in the CDRs gets recorded as blank.

- In this situation, CAR uses the default User ID of "_unspecified user" when it loads the CDRs, and the CDRs do not display in the Individual Bills User reports because no user by the name of "_unspecifieduser" exists in the Cisco Unified CM database.

If you look for the reports for a specific end user in the directory, either the User ID for that end user must be configured as the Owner User ID for the device, or that end user must have logged into the device with the extension mobility feature enabled.

Enhancements for Cisco Unified Reporting

SDL settings and the CtiID for Cisco CallManager and CTIManager on each server now display in the Unified CM Cluster Overview report under Unified CM Trace Information.

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

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 77](#)
- [Trusted List of IPs, page 78](#)
- [Allow Proxy, page 78](#)
- [Extension Mobility Cache Size, page 78](#)

Validate IP Address

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

The parameter 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 first gets 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 that are 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 gets checked against the list of devices that are 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 can perform login or logout.
- If the IP address is not found, the log in or log out attempt gets 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 that is 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 semicolons, 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, this means that EM log in and log out operations that use a web proxy are allowed.
- If the parameter specifies False, EM log in and log out requests that come from behind a proxy get rejected.

**Note**

The setting that 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 that extension mobility maintains. The minimum value for this field specifies 1000 and the maximum specifies 20000. The default specifies 10000.

**Note**

The value that you enter takes effect only if the [Validate IP Address](#) parameter specifies True.

Cisco Unified Reporting

The following list shows report data that is now available:

- SDL settings and CtiID for Cisco CallManager and Cisco CTIManager for each server display in the Unified CM Cluster Overview report under Unified CM Trace Information.

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

Cisco and Third-Party APIs

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

- [Cisco Unified TAPI, page 79](#)
- [Cisco Unified JTAPI, page 81](#)
- [Cisco Unified Communications Manager Configuration XML, page 83](#)
- [Cisco Unified Communications Manager Serviceability XML, page 97](#)

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, page 79](#)
- [Backward Compatibility Overview, page 80](#)
- [Join Across Lines Use Case, page 80](#)

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	<p>For A:</p> <p>CONNECTED</p> <p>CONFERENCED Caller=A, Called=B1, Connected=B1</p> <p>CONFERENCED Caller=A Called=C, Connected=C</p> <p>For B1:</p> <p>CONNECTED</p> <p>CONFERENCED Caller=A, Called=B1, Connected=A</p> <p>CONFERENCED Caller=B1 Called=C, Connected=C</p> <p>For B2:</p> <p>Call will go IDLE</p> <p>For C:</p> <p>CONNECTED</p> <p>CONFERENCED Caller=C, Called=B2, Connected=B1</p> <p>CONFERENCED Caller=C Called=A, Connected=A</p>

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 81](#)
- [Backward Compatibility Issues, page 83](#)
- [Backward Compatibility Issues, page 83](#)

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 functionality 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, page 83](#)
- [Added and Changed APIs, page 84](#)
- [Backward Compatibility Issues, page 85](#)
- [AXL Database APIs, page 85](#)

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 Q0NNQWRtaW5pc3RyYXRvcjpwjaXNjb19jaXNjbw==
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://ccmsvr/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 4](#) 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 4 *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 4 *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 5 provides information about the AXL database APIs. This table includes these designations:

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

Table 5 *AXL Database APIs*

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	5.1	5.1(2)	6.0	6.1		
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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 **AXL Database APIs (continued)**

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	5.1	5.1(2)	6.0	6.1		
removeIVRUserLocale	X	X	X	X	X	X	X	X	S	S	S	
updateIVRUserLocale	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 *AXL Database APIs (continued)*

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 *AXL Database APIs (continued)*

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 AXL Database APIs (continued)

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 5 *AXL Database APIs (continued)*

Operation	Cisco Unified Communications Release										UCR ¹	Description
	3.3	4.0	4.1	4.2	4.3	5.0d	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 6 provides information about the Serviceability SOAP API. This table includes these designations:

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

Table 6 *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
	selectCtlItem	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 6 Serviceability SOAP API Details (continued)

SOAP Service	Operation	Cisco Unified Communications Manager Release						UCR ¹
		3.0	4.0	4.3	5.0	6.0	6.1	
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.

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

Procedure

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

-
- Step 1** In the Select Product Category list, double-click **Voice and Unified Communications**.
- Step 2** In the Select Product list, double-click **Cisco Unified Communications Manager (CallManager)**.
- Step 3** From the Version drop-down list, select the Unified CM version train for which you want to see defects (for example, for Unified CM Release 6.1(2), select **6.1**).
- Step 4** Under Advanced Options, select **Use custom settings for severity, status, and others**.
- Step 5** In the options that display, click the **Open** check box to deselect that option.
Now, the only option that will get acted upon is the **Fixed** option.
- Step 6** Click **Search**.
-

**Tip**

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

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

Using Bug Toolkit

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

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

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

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

-
- Step 1** To access the Bug Toolkit, go to
<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>.
- Step 2** Log in with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field then, click **Go**.

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

Open Caveats

[Table 7](#) describes possible unexpected behaviors in Cisco Unified Communications Manager Release 6.1(2), which are sorted by component.

**Tip**

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

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

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

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

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

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

**Note**

Because defect status continually changes, be aware that [Table 7](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the “[Using Bug Toolkit](#)” section on page 99.

**Tip**

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

Table 7 Open Caveats as of April 21, 2008

Identifier	Headline
Component: AXL	
CSCso82375	Need profile type information in getDeviceProfilerresponse.
Component: CM Serviceability	
CSCsk96900	Unified CM SDI trace delete should be lower priority.
Component: Unified CM Docs	
CSCsh86972	Need exists for an alternative for AAR to allow TEHO / toll bypass / GW calls.
CSCtr84167	When you enable the service parameter "Block Offnet to Offnet Transfer" and make a blind transfer with Cisco Unity Connection, the Q.931 SETUP message which Cisco Unified Communications Manager sends to the PSTN gateway for an outbound PRI call still reaches the gateway. This transfer results in a dropped call.
Component: Unified CM CTI	
CSCsl36547	CTI heartbeat timeout; provider closing.
CSCsk93949	Don't get failure response when initiator park barged call on SIP phone
Component: Unified CM User Interface	
CSCso56349	If user changes to an unsupported RFC1123 hostname, no error displays.
CSCso78123	Unity Voice Mail Subscriber Templates missing from "Cisco Unity Voice Mail Information" frame under User Management -> User/Phone Add
CSCso71932	Unified Reporting Name Resolution reports error if DNS server mismatch
CSCso84603	When Application Server is Unity Connection: No selections in drop down menu for Application User Template. This must be selected to Create Cisco Unity Application User.
CSCso84730	Unable to configure ATA Speed Dials
CSCso85844	Changing to an unsupported hostname gives no error
Component: Call Processing	
CSCso82847	Digit Analysis: Applying External phone number mask gives '?'
CSCso28030	H323: Tandberg: H225D Line Control, Device Register messages for stopped session.
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.
CSCso66172	Media Control: Media layer not closing existing channel before opening a new channel
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: Ringback not heard for XEE.
CSCso82727	Media Control: CCM should not change Session ID for T.38 OLC in an H.323 to H.323 call

Table 7 *Open Caveats as of April 21, 2008*

CSCso29311	Media Control: No video displayed on Tandberg endpoints in ad-hoc conference
CSCsm45745	Media Control: Number of RTP Connections vary for different codecs.
CSCso67788	Media Control: Call failed from MeetingPlace 7.0 to H.323 video terminal
CSCso80890	Mobility: Mobile Voice Access Automatic Caller ID fails
CSCsm70455	QSIG: Unified CM does not honor reroute request from Matra PBX.
CSCso62633	SCCP: CTI application cannot retrieve a call redirected between nodes.
CSCso83057	SCCP: CUCM 6.1.1, DND set receive a call, causes feedback.
CSCsh97800	SCCP: Transfer cannot complete if phone answers an incoming call before the transfer completes.
CSCso68332	SCCP: SCCP phone connects whisper call for few ms when speaker is disabled
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.
CSCsh36576	System: Signaling DSCP from Unified CM incorrect for CS5, CS6, CS7, EF.
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.
CSCsh36576	System: CM 5.x - Signaling DSCP from CallManager incorrect for CS5, CS6, CS7, EF
Component: CPI	
CSCsi71487	Operating System: RTMT and perfmon counters show cimserver process memory consumption increases.
CSCsm25875	Operating System: Operations impacted after a single disk failure on a system with redundant disks.
CSCso57806	Platform API: Unified CM Release 6.1 software install prematurely shows "Status Complete", empty install log.
Component: Database	
CSCso47114	PMR 64860 - cdr check fail "Bad row id".
CSCso35247	Need exists for much faster database replication setup.
CSCso41720	PMR 44626 Replication setup failure occurs after upgrade ISAM error: deadlock.
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.
CSCso82088	utils dbreplication reset all fails.
CSCso69307	DMA install does not populate SIP Profile field on SIP Trunks
CSCso22817	PMR 64864 Repl setup fails; cdr check not able to delete extra rows

Table 7 **Open Caveats as of April 21, 2008**

Component: Directory	
CSCso30000	SSL LDAP authentication fails for Unified CM with AD 2003.
CSCso77371	DMA DirExport failed to migrate PersonalAddressBook
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: 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: SNMP Research Agent	
CSCso69839	sysName is not updated when hostname on CUCM server is changed
Component: TabSync	
CSCso12859	TabSync authentication fails with Unified CM if password contains '+' character.
Component: TAPISDK	
CSCsI31067	No LINE_MONITORTONE returned RecordWave with silence- Vista.
CSCso80785	After CCM upgrade from 4x to 6.x TSP client sends large userid to CTI

Documentation Updates

The *Updates to Cisco Unified Communications Manager 6.1(1) Documentation* document provides information about documentation omissions, errors, or updates that are not included in the documentation that supports the Unified CM 6.1 release train. To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/6_1_1/cucm-doc_updates-611.html

Obtaining Documentation and Submitting a Service Request

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)