Release Notes for Cisco Unified Communications Manager Release 7.0(2)

Updated April 22, 2010

Cisco Unified Communications Manager Release 7.0(2) addresses customer impacting issues that did not get resolved in Cisco Unified CM 7.0(1).

Table 1 Delta Between Release Notes for Unified CM 7.0(1) and Release Notes for Unified CM 7.0(2)

Additions and Changes
• Added the "Administrator Can Set User Credential Policy to Expire Without Making a Global Policy Change" section on page 159
• Added the "Considerations for LDAP Port Configuration" section on page 8
• Added the "Number of Digits Field Description is Incorrect" section on page 164
• Added the "Time-of-Day Routing Chapter Omits Information About Defined Time Periods" section on page 164
• Added the "Do Not Begin Starting and Ending Directory Numbers with a Zero (0)" section on page 164
• Updated the heading "Upgrading from Unified CM 6.0.(1) or Later to Unified CM 7.0(2) by Using the UCSInstall File" section on page 5
• Aded the "Use Microsoft Outlook to Receive Cisco Unified Communications Manager Licenses" section on page 8
• Added the "Cisco Unified Communications Manager Attendant Console Support in 7.0(2)" section on page 50
• Added the
• Deleted the "Attendant Console Chapter Incorrectly States that Attendant Console Installation is not Supported" section
• Added the "Important Notes for Cisco Unified CM Release 7.0(2)" section on page 7
• Updated the "Open Caveats for Cisco Unified Communications Manager Release 7.0(2) As of January 27, 2009" section on page 155

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

Table 1 Delta Between Release Notes for Unified CM 7.0(1) and Release Notes for Unified CM 7.0(2)

Additions and Changes
• Under Documentation Updates, added the "CAR Documentation Omits Information on Up and Down Arrows" section on page 113
• Added the "SIP Digest Username Length Limited to 32 Characters" section on page 178
•

These release notes include the release notes for Cisco Unified CM 7.0(1) as well as information specific to Unified CM 7.0(2) and discuss the following topics:

Note You can view the release notes for previous versions of Cisco Unified Communications Manager here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the "Important Notes for Cisco Unified CM Release 7.0" section on page 17 for information about issues that may affect your system.

Note To ensure continuous operation and optimal performance of your Cisco Unified Communications Manager system, you should upgrade to Cisco Unified Communications Manager 7.0(2).

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified Communications Manager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified Communications Manager system. For a list of commonly used URLs, see the "The Latest Software Upgrades for Unified CM 7.0 on Cisco.com" section on page 6.

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.

Cisco Unified Communications Manager Business Edition (Unified CMBE) offers you the features and functionality of Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection on one appliance platform.

System Requirements

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

Server Support

Cisco provides support for Cisco Unified CM Business Edition Release 7.0 on the MCS7828 server only.

Uninterruptible Power Supply

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

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

Upgrading to Cisco Unified Communications Manager 7.0(2)

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

Before You Begin

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

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

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

Important Upgrade Information

Do not upgrade Cisco Unified CMBE at the same time that the Cisco Unity Connection task Upgrade Database Statistics is running. Both processes are processor intensive, and allowing them to run simultaneously may cause the system to stop functioning and force you to restart the server.

By default, the Upgrade Database Statistics task runs at 3:30 am daily. To determine whether the task schedule has been changed, whether the task is currently running, and how long the task has recently taken to complete, log on to Cisco Unity Connection Administration. **Click Tools > Task Management > Update Database Statistics**.

The Task Definition Basics page displays a history of when the task started and when it completed. If the Time Started column has a value and the Time Completed column does not, the task is currently running.

If you must run the upgrade at a time that could overlap with the Upgrade Database Statistics task, reschedule the task to run before or after the upgrade. On the Task Definition Basics window for the task, click **Edit > Task Schedule**.

Do not reschedule the task to run during normal business hours. When the upgrade is complete, reset the schedule to the default settings.

Upgrade Paths to Cisco Unified Communications Manager 7.0(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

Ordering the Upgrade Media

To upgrade to Cisco Unified CM Release 7.0(2), use the Product Upgrade Tool (PUT) to obtain a media kit and license or to purchase the upgrade from Cisco Sales.

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

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

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

See the "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide*.

Upgrading from Unified CM 5.1(3) or Earlier

The following message displays when you attempt to upgrade from Unified CM 5.1(3) or earlier by using an SFTP/FTP server installed on Windows,

> "The directory was located and searched but no valid options or upgrades were available. Note, a machine cannot be downgraded so option and upgrade files for previous releases were ignored."

To correct this problem, perform the following steps.

Step 1 Use an SFTP server installed on UNIX/LINUX.

Step 2 Burn the unzipped directory to a DVD and perform a local DVD upgrade.

a. For example, if you upgrade from 5.1.3 to 7.0.2, unzip cisco-ipt-k9-patch7.0.2.10000-12.sgn.zip.

A new directory, cisco-ipt-k9-patch7.0.2.10000-12, now exists.

b. Copy this entire directory to the DVD.

c. F rom the "Software Installation/Upgrade" option, select **DVD/CD** as the source.

Upgrading from Unified CM 6.0.(1) or Later to Unified CM 7.0(2) by Using the UCSInstall File

Because of its size, the UCSInstall iso file, UCOS_7.0.2.10000-18.sgn.iso, comprises two parts:

- UCSInstall_UCOS_7.0.2.100000-18.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.2.100000-18.sgn.iso_part2of2

Procedure

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

Step 2 To reunite the two parts of the file, execute one of the following command.

Note Because the7.0.2.10000-18 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_7.0.2.10000-18.sgn.iso_part1of2 UCSInstall_UCOS_7.0.2.10000-18.sgn.iso_part2of2 > UCSInstall_UCOS_7.0.2.10000-18.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_7.0.2.10000-18.sgn.iso_part1of2+UCSInstall_UCOS_7.0.2.10000-18.sgn.iso_part2of2 UCSInstall_UCOS_7.0.2.10000-18.sgn.iso
```

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

5aeb0f01aeaa5bcb422a0307f0f4daba UCSInstall_UCOS_7.0.2.10000-18.sgn.iso

Upgrading From an Engineering Special

If you want to upgrade to Cisco Unified CM 7.0(2) and you are currently running an Engineering Special (ES), contact TAC to obtain the fixes that are included in the ES that you currently use.

The Latest Software Upgrades for Unified CM 7.0 on Cisco.com

You can access the latest software upgrades for Unified CM 7.0 on Cisco.com.

- Download Locale Installer, Personal Assistant, and Cisco Security Agent, page 6
- Download Phone Firmware, page 6

Download Locale Installer, Personal Assistant, and Cisco Security Agent

To download Unified Commuications Manager Updates, Locale Installer, Personal Assistant, and Cisco Security Agent, follow this procedure.

Procedure

Step 1 Go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Log in.

Step 3 In the window that displays, click **To access Voice Software downloads, click here**.

Step 4 From the Downloads window, click the "**+**" next to IP Telephony.

Step 5 From the options that display, click the "**+**" next to Call Control.

Step 6 From the options that display, click the "**+**" next to Cisco Unified Communication Manager (CallManager).

Step 7 From the options that display, click **Cisco Unified Communications Manager Version 7.0**.

- To download Unified CM 7.0 software, click **Unified Communications Manager Updates**. (Will be available for 7.1)
- To download Locale Installer, click **Unified Communications Manager/CallManager Locale Installer**.
- To download Upgrade Assistant, click **Unified Communications Manager/CallManager Upgrade Assistant**.
- To download Cisco Security Agent, click **Unified Communications Manager/CallManager Utilities**.

Download Phone Firmware

To download phone firmware, follow this procedure.

Procedure

Step 1 Go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Click **To access Voice Software downloads, click here**.

Step 3 From the Downloads window, click the "+" next to IP Telephony.

Step 4 From the options that display, click the "+" next to IP Phones.

Step 5 From the options that display, click the "+" next to Cisco Unified IP Phones 7900 Series.

Step 6 From the options that display, click the link for your phone.

Related Documentation

The view documentation that supports Cisco Unified CM Release 7.0(x), go to http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Cisco Unified Communications Manager System testing. The recommendations, which are not exclusive, represent an addition to interoperability recommendations for each individual voice application or voice infrastructure product.

For a list of software and firmware versions of IP telephony components and contact center components that were tested for interoperability with Cisco Unified Communications Manager 7.0(2) as part of Cisco Unified Communications System Release 7.0 testing, see

http://www.cisco.com/go/unified-techinfo

Note Be aware that the release of Cisco IP telephony products does not always coincide with Cisco Unified Communications Manager releases. If a product does not meet the compatibility testing requirements with Cisco Unified CM, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified CM Release 7.0(2). For the most current compatibility combinations and defects that are associated with other Cisco Unified CM products, refer to the documentation that is associated with those products.

Important Notes for Cisco Unified CM Release 7.0(2)

The following section contains information about caveats that Cisco Unified CM Release 7.0(2) resolves as well as other information important to users.

Considerations for LDAP Port Configuration

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

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

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

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

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

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

Use Microsoft Outlook to Receive Cisco Unified Communications Manager Licenses

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

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

Procedure

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

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

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

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

For More Information

"Licensing" chapter, *Cisco Unified Communications Manager System Guide*

ASCII Name Displays Instead of Unicode Name

Despite the fact that the User Locale configured on the device is Japanese on both IP phones, under the following conditions, the caller IP phone displays the called party name in English.

- In CallManager Service, the Always Display Original Dialed Number parameter is set to True; and
- The Default User Locale in the enterprise service parameter is set to English.

Workaround

- Change Always Display Original Dialed Number to False; or
- Change Default User Locale to Japanese.

Increase of Voice Mail Ports in Cisco Unified Communications Manager Administration

Cisco increased the number of voice mail ports that you can configure in Cisco Unified Communications Manager Administration. You can configure up to 999 ports, although the Cisco Unified Communications Manager Administration documentation states that you can configure a maximum of 144 ports.

Caveats Resolved in Unified CM 7.0(2)

Attendant Console

CSCsu54774 Line status info (CFA icon) not updated in real-time for AC client

CSCsv27446 Attendant Console calls stuck in queue, all calls routed to always route"

AXL

CSCsl26059 AXL logs show InvocationTargetException for requests.

CSCsw14260 getPhone AXL request throws error for Unified CM 7.0 phones with CAPF.

Backup-Resotre

CSCsv34475 Backup fails on Linux OpenSSH based SFTP servers.

BPS Bat

- CSCsr66309 Bulk administration update users value for fields to be ignored error exists in logs.
- CSCsr85564 BAT supercopy a phone template with Intercom configured make find error

- CSCsu00799 VG224 BAT error with shared lines.
- CSCsu43232 BAT does not restrict VG224 MAC address length.
- CSCsu64578 Find button near CSS is not available in BAT.
- CSCsu78938 An issue exists with consecutive recurring jobs in BAT.
- CSCsu90403 Generate phone reports window does not include "Forward All Destination".
- CSCsu95530 BAT.xlt file creates duplicate field entries when two line get configured.
- CSCsu97248 Cannot insert null into a null column, TelecasterSubscribedParameter.
- CSCsv07875 User cannot generate report on an H.323 gateway.
- CSCsw45780 UDP or phone template gets created with a SURL button and this button is assigned to a service. If a BAT add gets performed using this template and another service gets added at the same time via CSV, the SURL button can be incorrectly overwritten.
- CSCsw43113 BAT insert of SCCP VG224 does not add virtual endpoint.
- CSCsw72315 Missing data in phone report if there are more than 1500 phones.
- CSCsw86607 Insert 'Phones & Users fails inserting the phones in first try.

CAR

- CSCsv35554 From CAR > Bills > Department report, when user goes up in the report chain, "30029 Direct access to this screen is not allowed" displays.
- CSCsv39851 After a hostname gets changed, CAR fails to update the database URL.
- CSCsv47100 Changes made for Brazil DST.

CCM Serviceability

- CSCsw27176 Because the trace maximum number of files configured does not get enforced, LPM purging and alarms occur.

CDR Management

- CSCsv84484 When a user pushes CDR files to the SFTP server using GETFILE request, an exception occurs.

CLI

- CSCsr43052 CLI cannot handle file names that include a space.
- CSCsv13005 User cannot query SRV records from the platform CLI.
- CSCsv98921 CLI command **set account** stops at password.
- CSCsr43052 CLI cannot handle file names that include spaces.

CM CTI

- CSCsu72395 CTI SDL trace does not output DaReq and DaRes signals to/from DA.
- CSCsv18587 CTIManager should convert partition pkid to name before sending it to application.
- CSCsr94857 CTIManager IMS needs change notification when the LDAP Server gets updated.
- CSCsv47133 Acquiring device profiles puts CTI Manager into incorrect state.

CM UI

- CSCsr62036 Dependency for phone template should list extension mobility dynamic rec.

- CSCsr62247 MLA user with basic functionality can escalate their privledges.
- CSCsr64237 When user creates a personal address book entry, fast dials get created incorrectly.
- CSCsr70990 Logic to remove spaces in CiscoMOHSourceReport XML does not work.
- CSCsu02418 Saving CCMuser window device configuration resets user locale to None.
- CSCsu37723 OS Admin GUI Show > Hardware does not list serial number and BIOS information.
- CSCsu42245 When user attempts to add a directory number, this message : "Error: [1000] Invalid range for directory numbers" displays.
- CSCsu82769 Hold reversion ring and hold reversion notification interval is set to 0.
- CSCsu83698 From the crednetial policy in the GUI, user cannot uncheck the DoesNotExpire flag.
- CSCsu99802 If any text field on the Add End User window contains the string HREF the "Access to the requested resource has been denied. The attempted action was a violation of security protocols and will not be allowed. Please try another action" message displays.
- CSCsu96442 A CSS cannot be deleted, but there no dependency records exist for the CSS.
- CSCsv96037 License upload window does not fucntion for user with roles defined.
- CSCsm85167 When a new user created in AD tries to log in to WebDialer, a WebDialer window displays "Authentication failed. Please try again. User ID : null / Password : Blank."
- CSCsv07585 From the Device option on the CCMUser window, "User is not authorized to perform this function" message displays.
- CSCsx16330 Switch-version [nodatasync] option causes data loss on Unity Connection
- CSCsu74708 DN search returns incorrect output on devices with multiple lines.
- CSCsv99338 Route group does not display number of entries in "Max List Box Items."

Conversations

- CSCsv52480 Prompt for disabling message notification to a device is confusing.

Core

- CSCsv92357 In Unity Connection, scheduled tasks do not run.

Call Processing

- **Call Control**
  - CSCsr44298 Active call leak occurs due to disconnect during RSVP signaling.
  - CSCsv03084 CallControl should not generate CDR when a call is intercepted by the CallPickUp feature.
  - CSCsw27327 Unified CM crashes because of SsInvokeFeatureReq.
- **Datatbase**
  - CSCsu45290 Extension Mobility manager DND does not function when the icon is toggled from the assistant phone.
- **Digit Analysis**
  - CSCsv75285 Different partition pattern removed when park setting gets changed.
  - CSCsw77870 Unified CM route pattern does not match pattern correctly.
- **H323**
  - CSCsv36884 USer experiences fast busy when far end terminates call.

  - CSCsw91440 Unified CM does not support multirate bearer cap for speech calls.

- **Media Control**
  - CSCsr24661 H245interface sends MXInterfaceStoppedStreaming to wrong MediaExchange.
  - CSCsu02743 H.323 to H.323 FS calls fail to switch to T.38.
  - CSCsu88459 Unified CM does not respond to ""requestMode"" for T.38 from fax server.
  - CSCsv29679 IP-org caller gets disconnected if agent completes a transfer while the phone is ringing.
  - CSCsq92873 CUPC-H323-7985 call fails when 7985 exists in a non-default location.
  - CSCsu63550 Unified CM sends OLC before the TCS/MSD negotiation completes for transfer.
  - CSCsv74383 Unified CM should not inject null network or tsap address in OLC.
- **MGCP**
  - CSCsw20700 Unified CM MGCP PRI DMS-100 calling name display is missing.
  - CSCsv98384 Call gets rejected by H323 device due to missing mandatory IE (Bearer Capability).
- **Mobility**
  - CSCsr43770 CellProxy DaRes fails when RD matches pattern with potential matches.
  - CSCsr58797 The need exists for remote destination-CLID match to be done after CPN globalization.
  - CSCsu76962 Incoming call from remote destination number gets treated as external.
  - CSCsv16101 Call fails for remote destination on dual mode phone that is running SIP.
  - CSCsv32019 Locations bandwidth leaks when the Mobile connect feature gets used.
  - CSCsu56668 Single number reach fails intermittently on dual phone.
  - CSCsu81417 Call fails for remote destination on dual mode phone that is running SIP.
  - CSCsw41803 Forward unregistered does not work when RD calls its unregistered DN.
- **QSIG**
  - CSCsu78740 Call from IP phone to PBX extension fails when that PBX extension has a callforward configured to a PSTN extension.
  - CSCsu94361 PrCdpc leak occurs when DN is unroutable due to call intercept.
  - CSCsv21281 Calls can be picked up while CFNA is being processed.
  - CSCsr43219 QSIG diverted calls get sent with DivertingLegInformation2 Type of Number “Unknown” instead of the type of number configured in the Set Type of Number for Call Forward service parameter.
  - CSCsr50302 Unified CM does not display hungarian characters on an IP phone that is configured for the Hungarian locale.
  - .CSCsu54122 Blind transfer fails on QSIG link.
  - CSCsw28381 CT H323 QSIG trunk does not respect calling party selection.
- **SCCP**
  - CSCsu48651 Recording fails when it gets started by CTI too early.

  - CSCsu70206 Because the transfer button was pressed more than once, the StationCdpc does not clean up the LineCdpc process, so a memory leak occurs and all subsequent calls to this directory number fail.
  - CSCsw28285 Supervised transfer does not generate CMR for transfer-target.
  - CSCsw69164 Unified CM core at received StationLinetStatReq with large line index.
- **SIP Station**
  - CSCsu25841 Unified CM core dump occurs at SIPStation process when configuration gets changed.
  - CSCsw38654 Phone that is running SIP continues to play ringback after the call is answered.
- **SIP Trunk**
  - CSCsu56892 When a comma exists in a caller ID, calls do not reach SIP.
  - CSCsu97052 Unified CM does not wait for 183SDP prack before sending 200ok.
  - CSCsv52094 Unified CM includes SDP in ACK though SDP offer/answer finish in 183/PRACK.
  - CSCsw63783 ISDN Disconnect code 9F gets mapped to 31, Unspecified on SIP trunk connections. When a call is in an active state and disconnect cause 31 is received, the IP phone plays re-order.
  - CSCsr39929 SIP stack should escape the illegal characters passed by the application.
  - CSCsu10489 Blind transfer between Cisco IP Phone that is running SIP and Avaya fails.
  - CSCsw28126 SIP trunk stuck in Referpending state because of SIPcdpc leak.
  - CSCsw63146 TCP SIP timeout' parameter is not taken into account.
- **SS Callback**
  - CSCsu87562 Subsequent callback fails to Siemens PBX phone.
  - CSCsv64565 RTMT CallsInProgress counter constantly increases.
  - CSCsr65170 CBterm releases inbound call when CB monitor call gets released by PBX.
  - CSCsw50715 CallBackManager stuck in a loop and no dial tone is received.
- **SS Meet-Me**
  - CSCsr22343 Meet-Me Conference Manager cannot handle simultaneous Meet-Me Join requests.
- **Supplementary Services**
  - CSCsl01006 If a call occurs at the same time the call pickup group is updated, Unified CM cores.
  - CSCsv01929 Call pickup and call control get stuck in release intercept loop.
  - CSCsv03301 IP phone continues to ring after the call is forwarded.
  - CSCsv79496 CAC bandwidth allocation for recording.

CPI Certificate Management

- CSCsr68571 User cannot create SSL certificate with friendly hostname.
- CSCsv73904 After an upgrade, the user cannot access the Unified CM Admin/OS windows.

CPI OS

- CSCsr25966 Jstat, jps, and other java commands do not work properly.
- CSCso30000 SSL LDAP authentication fails for Unified CM with AD 2003.

CPI Service Manager

- CSCsk21012 ServM monitoring processes attempt to write to ummapped log files.

CUC Tomcat

- CSCsq32680 After an upgrade and switchover to the new partition or after a system restart, many services do not startm including Tomcat and Unified CM Administration. The web admin cannot be accessed, but the CLI can.

Curt

- CSCsr96714 In the Unified CM Cluster Report, Unified CM Component Version displays a mismatch in the components.

Database

- CSCsr29787 Database fails during upgrades for invalid (AXL) inserts like device profiles.
- CSCsr86876 Maximum Hunt Timer on hunt pilot cannot be set higher than 300.
- CSCsr91903 DRS restore of Unified CM database fails on new publisher server when it attempts to contact the subscriber servers.
- CSCsu77940 Extension Mobility logout or other notifications may be delayed for up to a minute.
- CSCsv07098 Digest user on third-party phone that is running SIP should not be allowed on other phones.
- CSCsr03923 CLID does not get sent in QSIG call.
- CSCsv92777 The replication status displays “2” even if the replication is broken.
- CSCsu98521 October Australian daylight saving changes.
- CSCsv47103 Missing lines in secondary A/A license cause SA problems.
- CSCsw50485 CUCM 7.x CFA, MWI fail due to autoregistrate busy loop on numplan table.
- CSCsv65196 Unity Connection 7.0 subscriber server with similar name to publisher server will not install.
- CSCsv83807 Unity Connection hostname change fails due to Informix not being fully online.
- CSCsv34676 Upgrade script does not update the systemversion.

Database Administration

- CSCsr68260 Application user device association for controlled devices does not get sorted.
- CSCsc48675 Inbound Redirecting Number IE Delivery should be selectable for QSIG.

Database IDS

- CSCsv56080 Update subscription on large number of UDPs does not work reliably.

Dialed Number Analyser

- CSCsq74372 Find button for Calling Search Space in DNA does not work.

Directory

- CSCso86593 A large amount of user data causes lost connection between DirSynch and Netscape LDAP.

CM Database

- CSCsr61658 User cannot delete the phone button templates.

Extension Mobility

- CSCsu39866 WDSysUser password gets sent in cleartext.
- CSCsv15437 Newly activated local extension mobility service does not get utilized by EMAp.
- CSCsv29965 Tomcat services do not start up properly due to EM service caching.
- CSCsv42719 Heavy extension mobility usage causes Tomcat to run out of threads.

IMS

- CSCso74471 Database communication error occurs when a user gets added on a subscriber server.
- CSCsr68519 User authentication on CCMUser window fails with "Failed to connect to LDAP Server" error. All Enduser authentication requests through the Tomcat web interfaces fail. LDAP directory or authentication configuration changes also fail indicating a null error.

IPMA Service

- CSCsr17062 IPMA does not work if the UserID contains a space.
- CSCsu90026 IPMA Assistant console cannot search if the search string includes spaces.
- CSCsv95210 IPMA login fails after DMA with an Invalid Username error.
- CSCsu04010 Issue with failover when Unified CM is hardbooted.

Media Storage Application

- CSCsr22819 SW MTP call-preservation does not terminate connection.
- CSCsu92735 Install log displays a warning stating that no valid wav file exists for audio source "SampleAudioSource."
- CSCsv34390 The IpVms media streaming driver encounters a shortage of large (8K) buffers that are used in streaming MOH and announcements. The IpVms media driver includes a "no free USR buffers" message in the system log.

Personal Directory

- CSCsv67277 (Japanese locale problem exists with common device configuration.

TAPI SDK

- CSCsu48465 Deadlock occurs when application attempts to add and remove observers back-to-back.
- CSCsv14475 Update the callinfo in CPIC if reason is PICKUP(in dialing state).
- CSCsu90986 Deadlock occurs when application attempts to add observers and remove observers from the address simultaneously.

QED

- CSCsv37730 Supported VICs differ between Unified CM 4.x and later.

QRT

- CSCsu63446 QRT xml does not get generated.

RTMT

- CSCsk86985 Service names differ between RTMT TCT and the trace configuration window.
- CSCsv47036 RTMT collects gzip traces files without closing them.

SDL

- CSCsr69611 Network services get blocked after heavy load.

Security

- CSCsv62484 CAPF database lookup should be case insensitive.

Serve Web Pages

- CSCsv19326 Billing server window hangs during add operation.

SMDI Service

- CSCsu78475 SMDI link server does not work.

Syslog

- CSCsr92354 After reboot, “Waiting on IPMI Initialization” message displays.

TAPI SDK

- CSCso97978 TSP configuration UI appears greyed out.

Telephony

- CSCsv02232 Unity Connection does not register correctly to Unified CM with NFT enabled.

Unknown

- CSCsm26758 Database tables out-of-sync do not trigger an alert.
- CSCso69307 DMA installation does not populate the SIP profile field on SIP trunks.
- CSCsq36823 CLI improperly displays query results.
- CSCsq38430 Cluster reboot should not be requiredafter a server gets deleted.
- CSCsq55224 User cannot add additional lines to the phones.
- CSCsq74528 After a DMA upgrade from Unified CM 4.1.3 to Unified CM 7.0, some of the original trace configuration settings get lost in the reset troubleshooting after upgrade.
- CSCsq92520 User cannot delete a user associated with a phone that is logged out.
- CSCsq95431 If notify client gets removed, MWI does not work.
- CSCsr02780 CLI does not object to **dbrep reset all** when **dbrep clusterreset** is running.
- CSCsr16701 Alarm 36 interferes with **reset all**.

Voice SIP Stack

- CSCsu88921 %SIP-3-NOMATCH: User cannot find matching CCB for ccCallID.
- CSCsu57129 When a SIP INVITE includes a From header that contains a comma, the INVITE is rejected with a 400 response.

- CSCsw69679 "." in the host portion of the URL causes call failure.

Important Notes for Cisco Unified CM Release 7.0

The following section contains information about caveats that the previous release of Cisco Unified CM Release 7.0 resolves.

Do Not Upgrade Cisco Unified CMBE When Cisco Unity Connection Upgrade Database Statistics Task is Running

Because both processes are processor intensive, if you allow them to run simultaneously the system may stop functioning and force you to restart the server.

The Upgrade Database Statistics task runs daily at 3:30 AM daily. To determine whether the task schedule has been changed, whether the task is currently running, and how long the task has recently taken to complete complete the following steps.

Step 1 Log on to Cisco Unity Connection Administration.

Step 2 Choose **Tools > Task Management >Update Database Statistics**.

The Task Definition Basics page displays a history of when the task started and when it completed. If the Time Started column has a value and the Time Completed column does not, the task is currently running.

Note If you need to run the upgrade at a time that could overlap with the upgrade database statistics task, reschedule the task to run before or after the upgrade. On the Task Definition Basics window for the task, click **Edit > Task Schedule**.

Do not reschedule the task to run during normal business hours. When the upgrade is complete, reset the schedule to the default settings.

Cisco Extension Mobility Feature Safe Enhancements Require Cisco Unified Communications Manager 7.0 Device Package

To use the functionality that is described in the "Cisco Extension Mobility Feature Safe" section on page 49 and in the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*, you must install the Cisco Unified Communications Manager 7.0 device package that supports Cisco Extension Mobility feature safe when it becomes available on the Cisco Unified IP Phone software download site. For information on how to access the device package, refer to the "Download Phone Firmware" section on page 6. For information on how to install the device package, refer to the readme document that posts with the device package on the software site.

Cisco Unified Communications Manager Attendant Console Plug-in

If you upgraded Cisco Unified Communications Manager to release 7.0(2), you can download the Cisco Unified Communications Manager Attendant Console plug-in. Cisco does not support the Cisco Unified Communications Manager Attendant Console with new installations of Cisco Unified Communications Manager 7.0(2), and the plug-in does not display in the Find and List Plugins window in Cisco Unified Communications Manager Administration.

If you reinstall Cisco Unified Communications Manager 7.0 on a server after an upgrade to 7.0, the Cisco Unified Communications Manager Attendant Console plug-in does not display in Cisco Unified Communications Manager Administration on that server after you install 7.0.

Cisco recommends that you save the plug-in to a location on a PC that you will remember in case you cannot access Cisco Unified Communications Manager Administration.

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.

Error 444 Displays When You Add or Edit Nokia s60 Devices After You Upgrade to Cisco Unified CM 7.0

Error 444 message displays in each of the two scenario circumstances that follow.

Circumstance 1

- You provision Nokia S60 devices by using the cmterm-nokia_s60_001-sccp.cp file.
- You upgrade your system to Unified CM 7.0.
- After the upgrade, attempts to add new Nokia S60 devices or edit existing Nokia S60 devices fail with error 444.

Circumstance 2

- You provision Nokia S60 devices by using the cmterm-nokia_s60_001-sccp.cp file.
- You upgrade your system to Unified CM 7.0.
- You install the newer cmterm-nokia_s60_2.0-sccp.cop file.
- You can add new Nokia S60 devices, but edits of Nokia S60 devices that were added before the upgrade still result in error 444.

Workaround

Follow one of these suggestions.

1. You can avoid these circumstances if you install the newer Nokia s60 cop file (cmterm-nokia_s60_2.0-sccp.cop) before you upgrade your system to Unified CM 7.0.
2. If the error message displays, you can perform the following tasks to ensure that you can configure Mobility Identity for the Nokia S60 device:
   a. In Cisco Unified Communications Manager Administration 7.0, disable auto-registration.
   b. 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**

   c. 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**.

   d. Reset all Nokia S60 devices.

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 by using the Logout button before making any changes in the user interface.

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.

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

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

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.

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.

Serviceability Not Always Accessible from OS Administration

In some scenarios, you cannot access 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.

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.

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 CM 4.x or 5.x to Cisco Unified Communications Manager 6.1(1x).

CSCsr95074 CLI Command to Set IOWAIT Threshold Added

Before you begin an upgrade, use RTMT , during off hours, to monitor the IOWAIT percentage. If it averages above 10 percent over 10 minutes, use the new CLI command **utils iothrottle threshold low <new iowait val>** to set the IOWAIT number to just above the 10-minute average.

Note If the average IOWAIT, as reported by RTMT, is below 10 percent, no need exists to execute a CLI command before the upgrade.

Three new CLI commands exist:

- **utils iothrottle threshold clear** clears the IOWAIT throttle value that is configured by **utils iothrottle threshold low** command.
- **utils iothrottle threshold low** sets the IOWAIT low threshold.
- **utils iothrottle threshold status** determines whether the IOWAIT threshold is set.

Note Your average IOWAIT should equal 1 to 2 percent.

Cisco CallManager Service Stops After Upgrade to Cisco Unified Communications Manager Release 7.0

After you upgrade to Cisco Unified Communications Manager 7.0 from a compatible Cisco Unified CM 5.X or 6.X release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated.

Immediately after you complete the upgrade to Cisco Unified Communications Manager 7.0, upload the software feature license that is required for Cisco Unified Communications Manager 7.0 in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 7.0.

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*.

CSCs096536—Cisco Extension Mobility Service Is Disabled, But You Can Still Get Service on Phone via Service URL

If you uncheck the Enable check box in the Phone Services Configuration window for the Cisco Extension Mobility service, restart the Cisco TFTP service, and reset the phone after you enable, configure, subscribe the phone to the Cisco Extension Mobility service, and add the service URL for the Cisco Extension Mobility service in Cisco Unified Communications Manager Administration, the phone displays the message, "Service not configured," although you can still see the Cisco Extension Mobility service and log in to the phone via the service URL.

To address this issue, perform one of the following tasks:

- Check the Enable check box in the Phone Services Configuration window for the Cisco Extension Mobility service.
- Remove the service URL for the Cisco Extension Mobility service.

After you perform the task, restart the Cisco TFTP service and reset the device for the changes to take effect.

Do Not Log On To the Console During Busy Hours

Cisco does not recommend logging on to the console during busy hours because additional CPU resources get consumed. This can lead to Code Yellow or Code Red alarms depending on the tasks that are being performed and the CPU that is utilized to perform those tasks. Cisco recommends that Console usage (remote or local) should get used to do maintenance or upgrades during Maintenance windows.

Important Information about Delete Transaction by 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* includes 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.

Resolving Interoperability Issues for Calling Party Normalization and Cisco Unity Connection

Cisco Unified Communications Manager 7.0 supports the international escape character +, as described in the "International Escape Character + Support" section on page 76; however, Cisco Unity Connection does not support this character. Because this application does not support the +, you must ensure that calls to Cisco Unity Connection do not contain the +, which ensures that voice-messaging features work as expected.

If you configure the + for the incoming prefix settings in Cisco Unified Communications Manager Administration to globalize the calling party number, the + gets inserted as a prefix to an incoming calling party number on a H.323, MGCP, or SIP gateway (or trunk, if applicable). If you configure calling party transformations, the device can localize the calling party number to transform the number to display differently than the globalized version. For example, a call from the North American Numbering Plan arrives as a 10-digit calling party number, 2225551234. Cisco Unified Communications Manager prefixes +1 to the calling party number to display the E.164 formatted number as +12225551234. On a phone in North America, Cisco Unified Communications Manager uses a calling party transformation to convert +12225551234 to 10 digits before the number displays on the phone; on a phone outside of North America, Cisco Unified Communications Manager may transform the number to only strip the + and to prefix the 00, as in 0012225551234.

For Cisco Unity Connection to work as expected, treat this application as a device and configure calling party transformations that ensure that the + does not get sent to this voice-messaging application. If the Cisco Unity Connection server uses a North American-based dial plan, localize the calling party number to NANP format before Cisco Unity Connection receives the calling party number. Because no calling party transformation options exist in Cisco Unified Communications Manager Administration for voice-messaging ports, make sure that you configure the calling party number transformations in the device pool that is associated with the voice-messaging ports. To localize the calling party number, also consider prefixing access codes, so the voice-messaging application easily can redial the number for certain features, such as Live Reply. For example, you can convert +12225551234 to 912225551234, and you can convert international number, +4423453456, to include the international escape code, 90114423453456.

For more information on localizing the calling party number, see the "Calling Party Normalization" section on page 44 and the "Calling Party Normalization" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Restoring Deleted Enterprise Cisco Unified IP Phone Services

Cisco Unified Communications Manager 7.0 automatically installs the following enterprise Cisco Unified IP Phone services during the Cisco Unified Communications Manager 7.0 installation/upgrade:

- Corporate Directory
- Intercom Calls
- Missed Calls
- Personal Directory
- Placed Calls
- Received Calls
- Voice Mail

You can customize, enable/disable, or delete these enterprise services, depending on the requirements for your system. For example, Cisco Unified Communications Manager disables the Intercom Calls service by default, but, if you want to do so, you can enable this service in the IP Phone Services Configuration window. Likewise, for example, you can update the Service URL field for the Corporate Directory service, so Cisco Unified Communications Manager points to your corporate directory server.

Cisco Unified Communications Manager Administration does not prevent you from deleting enterprise Cisco Unified IP Phone services. If you delete an enterprise Cisco Unified IP Phone service, you can restore the service by issuing the commands in Table 2 in the Command Line Interface (CLI). For information on how to start a CLI session, refer to *Command Line Interface Reference Guide for Cisco Unified Solutions*. For more information on Cisco Unified IP Phone services, refer to the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager System Guide*, and the "Enhanced IP Phone Services" section on page 73.

Tip You can only restore one service at a time. If you delete multiple services and want to restore more than one service, you must restore each service separately in the CLI.

Table 2 Restoring Standard Cisco Unified IP Phone Services

Enterprise Cisco Unified IP Phone Service	Command for Restoring Service
Corporate Directory	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('7eca2cf1-0c8d-4df4-a807-124b18fe89a4','Corporate Directory','Corporate Directory','Corporate Directory','Application:Cisco/CorporateDirectory',1,'t',6)
Intercom Calls	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('27f92f3c-11ed-45f3-8400-fe06431c0bfc','Intercom Calls','Intercom Calls','Intercom Calls','Application:Cisco/IntercomCalls',1,'f',4)
Missed Calls	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('d0059763-cdcc-4be7-a2a8-bbd4aac73f63','Missed Calls','Missed Calls','Missed Calls','Application:Cisco/MissedCalls',1,'t',1)

Table 2 Restoring Standard Cisco Unified IP Phone Services

Enterprise Cisco Unified IP Phone Service	Command for Restoring Service
Personal Directory	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('4a9d384a-5beb-4449-b176-cea0e8c4307c','Personal Directory','Personal Directory','Personal Directory','Application:Cisco/PersonalDirectory',1,'t',5)
Placed Calls	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('a0eed443-c705-4232-86d4-957295dd339c','Placed Calls','Placed Calls','Placed Calls','Application:Cisco/PlacedCalls',1,'t',3)
Received Calls	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('0061bdd2-26c0-46a4-98a3-48a6878edf53','Received Calls','Received Calls','Received Calls','Application:Cisco/ReceivedCalls',1,'t',2)
Voicemail	run sql insert into telecasterservice (pkid,Name,NameASCII,Description,URLTemplate,tkPhoneService,EnterpriseSubscription,Priority) values('ca69f2e4-d088-47f8-acb2-ceea6722272e','Voicemail','Voicemail','Voicemail','Application:Cisco/Voicemail',2,'t',1)

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, you must define a unique call park number or range of call park extension numbers for each partition in Cisco Unified Communications Manager Administration.

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.

Device Defaults Configuration Window Inaccurately Displays Only SCCP for the Cisco Unified IP Phone 7914 Expansion Module

Although the Device Defaults Configuration window in Cisco Unified Communications Manager Administration displays SCCP as the only supported protocol for the 7914 14-Button Line Expansion Module field, the Cisco Unified IP Phone Expansion Module can support either SCCP or SIP. For the 14-Button Line Expansion Module field, the default device load that displays in the Load Information field supports both protocols.

Viewing Privileges for Roles in Cisco Unified Communications Manager Administration

The Role Configuration window in Cisco Unified Communications Manager 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.

Serviceability Limitation When You Modify IP Addresses

When you modify the IP Address field, you cannot access the RTMT profiles, custom counters, custom alerts, and generic queries for Trace and 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 includes the 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 the 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.

Browser Requirements

The following browser requirements apply to Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Bulk Administration Tool, Cisco Unified Communications Operating System, Disaster Recovery System, and Cisco Unified Reporting:

- 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 these GUIs 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.

The preceding GUIs do not support the buttons or browser controls in your browser. Do not use the browser buttons or browser controls (for example, the Back button) when you perform configuration tasks.

Custom Background Images for Cisco Unified IP Phone 7906G and 7911G

Phone background images may not display properly on the Cisco Unified IP Phone 7906G and 7911G with languages that use large fonts, such as Chinese, Japanese, and Korean. To modify a background image for proper display, follow these guidelines:

- Use the following file sizes when you are creating PNG files for the locale:
  - 95x28 (full size image)
  - 23x8 (thumbnail image)

  Upload the image files to %TFTPPATH%\Desktops\95x28x1.
- Modify or create the List.xml file in the %TFTPPATH%\Desktops\95x28x1 folder to include the following lines, where image.png specifies the name of your image file:

  <CiscoIPPhoneImageList>

  <ImageItem Image="TFTP:Desktops/95x28x1/image.png"

  URL="TFTP:Desktops/95x28x1/image.png" />

  </CiscoIPPhoneImageList>

For more information, see the "Creating Custom Background Images" section in the *Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 7.0*.

Software Feature License

When you upgrade from an earlier release of Cisco Unified Communications Manager to Release 7.0(2), you must download and install a software feature license to activate the new features. For instructions about how to obtain and install a software feature license, see the "License File Upload" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Making Configuration Changes During an Upgrade

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration Changes

The administrator must not make any configuration changes to Cisco Unified Communications Manager during an upgrade. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option pages.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

For Cisco Unified Communications Manager Release 7.0(2), this restriction applies to upgrades from 4.x, 5.x, and 6.x releases.

For upgrades from Cisco Unified Communications Manager Release 4.x, you must discontinue all configuration activity before you run the Data Migration Assistant (DMA).

For upgrades from Cisco Unified Communications Manager Release 5.x and 6.x, you must discontinue all configuration activity before you upgrade to the new release by using either Cisco Unified Communications Operating System Administration or the Command Line Interface.

User Provisioning

For upgrades from Cisco Unified Communications Manager Release 4.x and 5.x, any provisioning that the end user performs to user-facing features after the upgrade begins could get lost.

For upgrades from Cisco Unified Communications Manager Release 6.x, changes that are made to the following user-facing features get preserved after the upgrade completes:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication
- Recording enabling
- Single Number Reach enabling

Cisco Firmware Update CD (FWUCD)

The Cisco Firmware CD is updated periodically. You can find information and download the CD from http://tools.cisco.com/support/downloads/go/InterfaceModuleSWT.x?mdfid=281941895&mdfLevel=null&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+7.0&treeMdfId=278875240&hybrid=Y&imst=N.

To see the latest FWUCD,

1. Click the link above.
2. Click **Unified Communications Manager/CallManager Utilities**.
3. Under Latest Release, click **Firmware 2.1**.

   The updates are listed.

The readme file lists all of the caveats that are resolved in the firmware update.

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

New and Changed Information

No new and changed information exists for Unified CM 7.0(2).

The following section contains information that is new or changed for the 7.0 release of Cisco Unified Communications Manager.

- Installation, Upgrade, Migration, and Disaster Recovery, page 30

Installation, Upgrade, Migration, and Disaster Recovery

This following sections describe the changes that were made to the installation, upgrade, and disaster recovery procedures in Cisco Unified Communications Manager 7.0(x):

Disaster Recovery System

In Release 7.0, 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*.

Installation, Upgrade, and Replacement

This section contains information about installation, upgrade, and replacement changes for this release:

- The Apply a Patch option of the installation program now supports applying full patch ISO upgrade patch file, in addition to the previously supported ES and SU patch types.
- If you restore Cisco Unified Communications Manager on a server on which you previously installed COP file enablers for new device types or locales, you must reinstall those COP file enablers after installation.

Cisco Unified Communications Operating System Administration

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

Show IP Preferences

Cisco Unified Communications Operating System Administration contains a new window that displays a list of registered ports that the system can use. For a description of the fields in the IP Preferences window, see Table 3.

Table 3 IP Preferences Field Descriptions

Field	Description
Application	Name of the application that is using (listening on) the port.
Protocol	Protocol that is used on this port (TCP, UDP, and so on).
Port Number	Numeric port number.
Type	Type of traffic that is allowed on this port: • Public—All traffic that is allowed • Translated—All traffic that is allowed but forwarded to a different port • Private—Traffic only allowed from a defined set of remote servers.
Translated Port	Traffic destined for this port gets forwarded to the port that is listed in the Port Number column. This field applies to Translated type ports only.
Status	Status of port usage: • Enabled—In use by the application and opened by the firewall • Disabled—Blocked by the firewall and not in use
Description	Brief description of how the port is used.

GUI Changes

To access the IP Preferences window from the Cisco Unified Communications Operating System Administration window, choose **Show > IP Preferences**.

For More Information

Refer to the *Cisco Unified Communications Operating System Administration Guide*.

Command Line Interface

This section provides information about the following CLI commands that are new or changed for Cisco Unified Communications Manager Release 7.0(x). For more information about command syntax and parameters, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

- **set cli pagination {on | off}**

  For the current CLI*Cisco Unified Communications Manager Bulk Administration Guide* session, this command turns automatic pagination **On** or **Off**.

- **show cli pagination**

  This command displays the status of automatic CLI pagination.

- **set network hostname** *hostname*

  This commands sets the network host name and then causes a restart of the system.

Caution This command causes the system to restart.

Note The host name must follow the rules for ARPANET host names. It must start with an alphabetic character, end with an alphanumeric character, and comprise alphanumeric characters and hyphens. Ensure the host name does not exceed a maximum length of 63 characters.

- **utils ntp start**

  If NTP is not already running, this command starts it.

- **utils ntp restart**

  This command restarts the NTP service.

- **utils system boot {console | serial | status}**

  This commands redirects where the system boot output gets sent.

- **utils system upgrade initiate**

  This command starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file.

- **utils create report csa**

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

- **utils snmp hardware-agents stop**

  This command stops all SNMP agents that the hardware vendor provides.

- **show network ipprefs {all | enabled | public}**

  This command displays the list of ports that have been requested to be opened or translated in the firewalls. For a description of the show **network ipprefs command** output, see the "Show IP Preferences" section on page 31.

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

Tip For information on browser requirements, see the "Browser Requirements" section on page 27.

New and Updated Enterprise and System Parameters

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

Enterprise Parameters

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

- Show Manager Name in Directory—Supports functionality for the Cisco Unified CM User Options.
- Show User ID Name in Directory—Supports functionality for the Cisco Unified CM User Options.

Service Parameters

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

- Show Line Group Member DN in finalCalledPartyNumber CDR Field—Supports the Cisco CallManager service for CDR and CMR (requires that you click the Advanced button to display).
- Add Incoming Number Prefix to CDR—Supports the Cisco CallManager service for calling party normalization for CDR and CMR (requires that you click the Advanced button to display).
- BLF Pickup Audio Alert Setting of Idle Station—Supports Cisco CallManager service for the BLF Pickup feature
- BLF Pickup Audio Alert Setting of Busy Station—Supports Cisco CallManager service for the BLF Pickup feature

- Forward Maximum Hop Count—Supports Cisco CallManager service for the call forward all loop prevention and breakout feature.
- Incoming Calling Party National Number Prefix - MGCP, Incoming Calling Party International Number Prefix - MGCP, Incoming Calling Party Subscriber Number Prefix - MGCP, Incoming Calling Party Unknown Number Prefix - MGCP—Supports Cisco CallManager service for the calling party normalization feature (requires that you click the Advanced button to access).
- Incoming Calling Party National Number Prefix - H.323, Incoming Calling Party International Number Prefix - H.323, Incoming Calling Party Subscriber Number Prefix - H.323, Incoming Calling Party Unknown Number Prefix - H.323—Supports Cisco CallManager service for the calling party normalization feature (requires that you click the Advanced button to access).
- Incoming Calling Party Unknown Number Prefix - SIP—Supports Cisco CallManager service for the calling party normalization feature (requires that you click the Advanced button to access).
- Strip + on Outbound Calls—Supports Cisco CallManager service for the calling party normalization feature
- Fail Call If Trusted Relay Point Allocation Fails—Supports Cisco CallManager service for trusted relay points.
- DSCP for G.Clear Calls—Supports Cisco CallManager service for the G.Clear codec.
- DSCP for Priority G.Clear Calls (represents the specific MLPP value EF DSCP [101101])—Supports Cisco CallManager service for the G.Clear codec.
- DSCP for Immediate G.Clear Calls (represents the specific MLPP value EF DSCP [101100])—Supports Cisco CallManager service for the G.Clear codec.
- DSCP for Flash G.Clear Calls (represents the specific MLPP value EF DSCP [101001])—Supports Cisco CallManager service for the G.Clear codec.
- DSCP for Flash Override G.Clear Calls (represents the specific MLPP value EF DSCP [101010])—Supports Cisco CallManager service for the G.Clear codec.
- DSCP for Executive Override G.Clear Calls (represents the specific MLPP value EF DSCP [101010])—Supports Cisco CallManager service for the G.Clear codec.
- G. Clear Bandwidth Override—Supports Cisco CallManager service for the G.Clear codec.
- SIP Route Class Naming Authority—Supports Cisco CallManager service for the G.Clear codec.
- SIP Clear Channel Data Route Class Label—Supports Cisco CallManager service for the G.Clear codec.
- Choose Encrypted Audio Conference Instead of Video Conference—Supports Cisco CallManager service for the Intelligent Bridge Selection feature.
- Minimum Video-Capable Participants to Allocate Video Conference—Supports Cisco CallManager service for the Intelligent Bridge Selection feature.
- Allocate Video Conference Bridge for Audio-only Conferences when Video Conference Bridge has Higher Priority—Supports Cisco CallManager service for the Intelligent Bridge Selection feature.
- Play Secure Indication Tone—Supports Cisco CallManager service for the secure tone indication feature.

Menu Changes

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

Main Window

If you have a Cisco Unified Presence server that is configured as part of the Cisco Unified Communications Manager, the main Cisco Unified Communications Manager Administration window displays a link to the Cisco Unified Presence publisher server.

To access Cisco Unified PresenceAdministration, click the link to the Cisco Unified Presence publisher server.

System

The System menu provides the following new settings:

- System > Device Pool—New settings include Local Route Group, Calling Party Transformation CSS, Called Party Transformation CSS, Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix.
- System > LDAP > ...—This setting remains configurable for Cisco Unified Communications Manager Business Edition 7.0
- System > MLPP > Domain—This menu path replaces System > MLPP Domain, which was used in earlier releases.
- System > MLPP > Namespace > Resource Priority Namespace Network Domain (or Resource Priority Namespace List)—New windows display.
- System > Security Profile > CUMA Server Security Profile—New settings for this new profile include Name, Description, Device Security Mode, Transport Type, and X.509 Subject Name.
- System > Application Server—New settings display for URL, End User URL, and Selected Application User.

Call Routing

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

- Call Routing > Route/Hunt > Hunt List (Add the hunt list; after you click Save, the Add a Route Group button displays. To display the Route List Detail Configuration window, click the Add a Route Group button.)—New setting that is called Calling Party Number Type displays in Route List Detail Configuration window.

- Call Routing > Route/Hunt > Route Pattern—New settings that are called Calling Party Number Type and Resource Priority Namespace Network Domain display.
- Call Routing > Route/Hunt > Hunt Pilot—New setting that is called Calling Party Number Type displays.
- Call Routing > Intercom > Intercom Translation Pattern—The Urgent Priority check box gets updated to allow you to check or uncheck the check box, depending on your configuration preferences.
- Call Routing > Class of Control > Access List—This menu option moved from the Device menu to the Call Routing menu.
- Call Routing > Class of Control > Time Period—New settings that are called Owner ID and Published to End Users display.
- Call Routing > Class of Control > Time Schedule—New settings that are called Category, Owner ID, and Published to End Users display.
- Call Routing > Translation Pattern——New settings that are called Calling Party Number Type and Resource Priority Namespace Network Domain display; the Urgent Priority check box gets updated to allow you to check or uncheck the check box, depending on your configuration preferences.
- Call Routing > Transformation Pattern > Calling Party Transformation Pattern—New window displays; new settings that are called Calling Party Number Type, Calling Party Numbering Plan, Calling Party Transformation CSS, and Discard Digit Instructions display.

Media Resources

The Media Resources menu displays the following new and updated settings.

- Media Resources > Annunciator—New setting that is called Use Trusted Relay Point displays.
- Media Resources > Conference Bridge—New setting that is called Use Trusted Relay Point displays.
- Media Resources > Media Resource Group—The Reset button no longer displays.
- Media Resources > Media Resource Group List—The Reset button no longer displays.
- Media Resources > Media Termination Point—New setting that is called Trusted Relay Point displays.
- Media Resources > Music On Hold Server—New setting that is called Use Trusted Relay Point displays.
- Media Resources > Transcoder—New setting that is called Trusted Relay Point displays.

Voice Mail

The Voice Mail menu displays the following new and updated settings.

- Voice Mail > Voice Mail Port Wizard—The External Number Mask field allows you to enter the international escape character +.
- Voice Mail > Cisco Voice Mail Port—The External Number Mask field allows you to enter the international escape character +.
- Voice Mail > Voice Mail Pilot—The Voice Mail Pilot Number field allows you to enter the international escape character +.

Device

The Device menu displays the following new and updated settings.

- Device > CTI Route Point—New settings that are called Use Trusted Relay Point, Calling Party Transformation CSS, and Use Device Pool Calling Party Transformation CSS display.
- Device > Gateway—New settings that are called Use Trusted Relay Point, Calling Party Transformation CSS, Use Device Pool Calling Party Transformation CSS, Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix display.
- Device > Phone—New settings that are called Services Provisioning, Use Trusted Relay Point, BLF Audible Alert Setting (Phone Idle), BLF Audible Alert Setting (Phone Busy), Calling Party Transformation CSS, Use Device Pool Calling Party Transformation CSS, Protected Device, Associated Mobility Identity, Add New Mobility Identity, Associated Remote Destinations, and Add a New Remote Destination display.
- Device > Trunk—New settings that are called Use Trusted Relay Point, Calling Party Transformation CSS and Use Device Pool Calling Party Transformation CSS, Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix display.
- Device > Trunk > SIP Trunk configuration—New settings that are called SRTP Allowed, Remote-Party-Id, Asserted-Identity, Asserted-Type, and SIP Privacy display.
- Device > Remote Destination—New settings that are called Cisco Unified Mobile Communicator, Dual Mode Phone, and all fields in the new When Mobile Connect Is Enabled pane display. The following settings no longer display: Allowed Access List, Blocked Access List, Smart Client Installed.
- Device > Device Settings > Access List—This menu item has moved to the Call Routing menu as the Call Routing > Class of Control > Access List menu option.
- Device >Device Settings >SIP Profile——New setting that is called Resource Priority Namespace List displays.
- Device > Device Settings > Common Device Configuration—New setting that is called Use Trusted Relay Point displays.

Application

No updates or new fields exist for this menu.

User Management

The User Management menu provides the following updates:

- User Management > End User—The Access Lists setting got removed from the Mobility Information pane.

Bulk Administration

The Bulk Administration menu supports the following updates:

- Bulk Administration > Mobility >Time of Day Access—New submenu allows you to insert, delete, and export Time of Day Access though the Bulk Administration Tool.
- Bulk Administration > Import/Export> Validate Import File—New submenu allows you to validate the import file while you import configuration through the Bulk Administration Tool.

Cisco Unified Communications Manager Features and Applications

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

Busy Lamp Field 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 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 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).

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 phones that 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 connects to one of these phones.

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 does not receive BLF notifications. See "Configuring and Applying the SUBSCRIBE Calling Search Space" for more information.

See "Cisco Unified Communications Manager Administration Configuration Tips" section on page 39 for more information about configuring call pickup groups, calling search spaces, and hunt pilots to support the BLF Pickup feature.

Cisco Unified Communications Manager Administration Configuration Tips

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 on the server for the BLF Pickup feature on supported phones.
- The calling search space for the monitoring DN must contain the partition of the monitored DN, or call pickup will fail. See "Using Call Pickup Features with Partitions to Restrict Access" for more information.

- 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 SpeedDial but do not associate the pickup groups, the phone receives BLF call alerts, but the user hears reorder 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 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 gets 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 vonfiguration 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 setting controls the audio alert for BLF pickup when the phone is idle (not in use). The Off setting disables the alert, the On setting enables the alert (play tone), and the Default setting uses the BLF Pickup Audio Alert Setting of Idle Station service parameter (see the "New and Updated Enterprise and System Parameters" section on page 33).
- BLF Audible Alert Setting (Phone Busy)—This setting controls the audio alert for BLF pickup when the phone is busy. The Off setting disables the alert, the On setting enables the alert (play tone), and the Default setting uses the BLF Pickup Audio Alert Setting of Busy Station service parameter setting (see the "New and Updated Enterprise and System Parameters" section on page 33).

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 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 for this required field. Default: 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 for this required field. Default: 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.

Serviceability Considerations

No changes for serviceability exist for this 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.

CAR/CDR Considerations

No changes for CAR and CDRs exist for this feature.

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.

- Press the BLF Pickup button when the BLF status is idle (or busy) to initiate an outgoing SpeedDial. 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 call pickup, press the BLF Pickup button when the BLF status is alerting.

This feature adds a flashing “alerting” status icon (see the following example) 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 Cisco Unified CM User Options 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*

Call Forward All Loop Prevention and Breakout

Cisco Unified Communications Manager prevents Call Forward All activation on the phone when a Call Forward All loop is identified. For example, Cisco Unified Communications Manager identifies a call forward loop when the user presses the CFA softkey on the phone with directory number 1000 and enters 1001 as the CFA destination, and 1001 has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1003, which has forwarded all calls to 1000. In this case, Cisco Unified Communications Manager identifies that a loop occurs and prevents CFA activation on the phone with directory number 1000.

Call Forward All loops do not impact call processing because Cisco Unified Communications Manager supports CFA loop breakout, which ensures that if a CFA loop is identified, the call goes through the entire forwarding chain, breaks out of the Call Forward All loop, and completes as expected, even if CFNA, CFB, or other forwarding options are configured along with CFA for one of the directory numbers in the forwarding chain. For example, the user for the phone with directory number 1000 forwards all calls to directory number 1001, which has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1000, thus creating a CFA loop. In addition, directory number 1002 has configured CFNA to directory number 1004. The user at the phone with directory number 1003 calls directory number 1000, which forwards to 1001, which forwards to 1002. Cisco Unified Communications Manager identifies a CFA loop, and the call, which breaks out of the loop, tries to connect to directory number 1002. If the No Answer Ring Duration timer expires before the user for the phone with directory number 1002 answers the call, Cisco Unified Communications Manager forwards the call to directory number 1004.

For a single call, Cisco Unified Communications Manager may identify multiple Call Forward All loops and attempts to connect the call after each loop is identified.

Cisco Unified Communications Manager Administration Configuration Tips

If Call Forward All activation occurs in Cisco Unified Communications Manager Administration or the Cisco Unified Communications Manager User Options, Cisco Unified Communications Manager does not prevent the CFA loop.

If the same directory number exists in different partitions, for example, directory number 1000 exists in partitions 1 and 2, Cisco Unified Communications Manager allows the CFA activation on the phone.

Cisco Unified Communications Manager prevents Call Forward All loops if CFA is activated from the phone, if the number of hops for a Call Forward All call exceeds the value that is specified for the Forward Maximum Hop Count service parameter, and if all phones in the forwarding chain have CFA activated [not Call Forward Busy (CFB), Call Forward No Answer (CFNA), or any other call forwarding options]. For example, if the user with directory number 1000 forwards all calls to directory number 1001, which has CFB and CFNA configured to directory number 1002, which has CFA configured to directory number 1000, Cisco Unified Communications Manager allows the call to occur because directory number 1002 acts as the CFB and CFNA (not CFA) destination for directory number 1001.

GUI Changes

If you do not want to use the default value, configure the Forward Maximum Hop Count service parameter. See the "New and Updated Enterprise and System Parameters" section on page 33.

Service Parameter and Enterprise Parameter Changes

The Forward Maximum Hop Count service parameter, which supports the Cisco CallManager service, specifies the maximum number of call hops that can occur for a Call Forward All chain; for example, if the value of this parameter equals 7, and a Call Forward All chain occurs consecutively from directory numbers 1000 to 1007, which equals 7 hops, Cisco Unified Communications Manager prevents a phone user with directory number 2000 from activating CFA to directory number 1000 because no more than 7 forwarding hops are supported for a single call. For more information on this service parameter, including special considerations for calls that use Q.SIG trunks, click the Forward Maximum Hop Count link in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.0, you can configure call forward all loop prevention and breakout.

Serviceability Considerations

The call forward all loop prevention and breakout feature relies on the Cisco CallManager service, so activate this service in Cisco Unified Serviceability.

User Tips

If the phone user activates Call Forward All in Cisco Unified CM User Options, Cisco Unified Communications Manager does not prevent the CFA loop.

For More Information

- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*

Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without modifying the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Tip Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

Cisco Unified Communications Manager Administration Configuration Tips

The calling party number that displays for a shared line depends on the sequence of call control events in Cisco Unified Communications Manager. To avoid displaying an incorrect localized calling party number on a shared line, especially when the shared line occurs in different geographical locations, make sure that you configure the same Calling Party Transformation CSS for different devices that share the same line.

SIP trunks and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the gateway strips the + when Cisco Unified Communications Manager sends the call information to the gateway.

SIP does not support the number type, so calls through SIP trunks only support the Incoming Calling Party Unknown Number Prefix settings.

A QSIG configuration usually supports a uniform dial plan. Transformation of numbers and prefixes may cause feature interaction issues if you have use QSIG.

For localizing the calling party number, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

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

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

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

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

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

If you do not configure a colon (:) in the incoming prefix fields, Cisco Unified Communications Manager does not strip any digits from the calling party number.

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

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

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

GUI Changes

The following changes to the GUI apply:

- Calling Party Number Type—Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. In the following windows in Cisco Unified Communications Manager Administration, you can configure the Calling Party Number Type setting: Route List Detail Configuration (Call Routing > Route/Hunt > Hunt List; Add the hunt list; after you click **Save**, the Add a Route Group button displays. To display the Route List Detail Configuration window, click the **Add a Route Group** button.), Route Pattern Configuration (Calling Routing > Route/Hunt > Route Pattern), Hunt Pilot Configuration (Calling Routing > Route/Hunt > Hunt Pilot), Translation Pattern Configuration (Call Routing > Translation Pattern), and Calling Party Transformation Pattern Configuration (Call Routing > Transformation Pattern > Calling Party Transformation Pattern).
- Incoming Calling Party National Number Prefix—Used for globalizing the calling party number, Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), colon (:), or the pound sign (#). When the prefix in this parameter is applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions that pertain to the call, such as supplementary services

including call forwarding, call park, voice messaging, CDR data, and so on. This setting displays in the following windows in Cisco Unified Communications Manager Administration: Device Pool (System > Device Pool), Service Parameter (System > Service Parameters), Gateway (Device > Gateway), Trunk (Device > Trunk).

- Incoming Calling Party International Number Prefix—Used for globalizing the calling party number, Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), colon (:), or the pound sign (#). When the prefix in this parameter is applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions that pertain to the call, such as supplementary services including call forwarding, call park, voice messaging, CDR data, and so on. This setting displays in the following windows in Cisco Unified Communications Manager Administration: Device Pool (System > Device Pool), Service Parameter (System > Service Parameters), Gateway (Device > Gateway), Trunk (Device > Trunk).
- Incoming Calling Party Subscriber Number Prefix—Used for globalizing the calling party number, Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), colon (:), or the pound sign (#). When the prefix in this parameter is applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions that pertain to the call, such as supplementary services including call forwarding, call park, voice messaging, CDR data, and so on. This setting displays in the following windows in Cisco Unified Communications Manager Administration: Device Pool (System > Device Pool), Service Parameter (System > Service Parameters), Gateway (Device > Gateway), Trunk (Device > Trunk).
- Incoming Calling Party Unknown Number Prefix—Used for globalizing the calling party number, Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), colon (:), or the pound sign (#). When the prefix in this parameter is applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions that pertain to the call, such as supplementary services including call forwarding, call park, voice messaging, CDR data, and so on. This setting displays in the following windows in Cisco Unified Communications Manager Administration: Device Pool (System > Device Pool), Service Parameter (System > Service Parameters), Gateway (Device > Gateway), Trunk (Device > Trunk).
- Calling Party Transformation CSS—This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

  Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

  All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration can localize the calling party number for themselves; therefore, you can access this setting in the following windows in Cisco Unified Communications Manager Administration: Phone (Device > Phone), CTI Route Points (Device > CTI Route Point), Gateway (Device > Gateway), Trunk (Device > Trunk), Remote Destination Profile (Device > Device Settings > Remote Destination Profile)

- Use Device Pool Calling Party Transformation CSS—To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the device configuration window. All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration can localize the calling party number for themselves; therefore, you can access this setting in the following windows in Cisco Unified Communications Manager Administration: Phone (Device > Phone), CTI Route Points (Device > CTI Route Point), Gateway (Device > Gateway), Trunk (Device > Trunk), Remote Destination Profile (Device > Device Settings > Remote Destination Profile)

Service Parameter and Enterprise Parameter Changes

Calling party normalization service parameters support the Cisco CallManager service, so before you configure calling party normalization, activate the Cisco CallManager service in Cisco Unified Serviceability. To locate the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**; choose the server and the Cisco CallManager service. After the parameters display, click **Advanced**. For information on the service parameter, click the hyperlink for the service parameter name or the question mark that displays in the upper, right corner of the window. The following service parameters support calling party normalization (globalization of the calling party number):

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

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.0, you can configure calling party normalization.

Serviceability Considerations

Calling party normalization relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

BAT Considerations

You can configure the Calling Party Transformation CSS and Use Device Pool Calling Party Transformation CSS in BAT. You can also configure the incoming prefix settings.

CAR/CDR Considerations

For information on CAR support, see the "Cisco Unified Communications Manager CDR Analysis and Reporting" section on page 112.

For information on CDR support, see the "Cisco Unified Communications Manager Call Detail Records" section on page 118.

User Tips

Cisco Unified IP Phones 7906, 7911, 7931, 7961, 7962, 7965, 7970, 7971, and 7975 support calling party normalization. Depending on your configuration, a phone user may not need to edit the call log directory entry on the phone before placing a call. Depending on your configuration, the phone user may see the international escape character, +, in the call log directories on the phone.

For More Information

- Non-Urgent Translation Patterns, page 88
- "Calling Party Normalization," *Cisco Unified Communications Manager Features and Services Guide*
- "Device Pool Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route List Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Understanding Route Plans," *Cisco Unified Communications Manager System Guide* (contains information on the international escape character +)

Cisco Emergency Responder Location Management Support in Application Server Configuration Window

Description

Cisco Unified Communications Manger 7.0 supports off-premise emergency call support in Cisco Emergency Responder 7.0.

Cisco Emergency Responder 7.0 supports Intrado V9-1-1 for Enterprise Service in the Cisco Unified Communications environment. If you subscribe to IntradoV9-1-1 for Enterprise Service, you can use Cisco Emergency Responder (ER) to simplify emergency call management. Cisco ER provides an interface that allows you to enter and synchronize on-premise and off-premise phone location information directly to the Intrado database. Cisco ER works in conjunction with Intrado to provide emergency services to phones that are located on the corporate network (on premise) and phones that are located away from the corporate network (off premise).

You must enable the Cisco Emergency Responder Location Management service in the Application Server Configuration in Cisco Unified Communications Manager Administration. When you enable the CER Location Management application, you enter the name that displays in the navigation drop-down box in the Cisco Unified CM User Options and the URL to the Cisco Emergency Responder Off-Premise window. In the Cisco_ER Off-Premise window, users can enter in their location information.

Users with off-premise phones cannot make emergency calls until they enter their location and associate this information with their directory number. After the location information is verified, emergency calls that are placed from off-premise phones can complete.

Cisco Unified Communications Manager Administration Configuration Tips

This feature requires you to enable Cisco Emergency Responder Location Management service in the Application Server Configuration in Cisco Unified Communications Manager Administration.

User Tips

See the *Cisco Emergency Responder Off-Premise Location Management User Guide*.

For More Information

- *Cisco Emergency Responder Administration Guide 7.0*

Cisco Extension Mobility Feature Safe

Tip In addition to reviewing the following section, see the "Cisco Extension Mobility Feature Safe Enhancements Require Cisco Unified Communications Manager 7.0 Device Package" section on page 18.

Cisco Extension Mobility (EM) equivalency eliminates the phone-model dependency of phone button templates. The following factors determine the model equivalency among the various phones:

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

EM equivalency includes the following support feature for the Cisco Unified IP Phones:

- Feature Safe on Phone Button Template—Phones can use any phone button template that has the same number of line buttons that the phone model supports.

Release 7.0(x) of Cisco Unified Communications Manager enhances the existing Extension Mobility (EM) equivalency mechanism. The equivalency enhancement works across phone types as follows:

- 7940 SCCP, 7941 SCCP, 7942 SCCP, and 7945 SCCP models, which are equivalent, can share an EM profile.
- 7940 SIP, 7941 SIP, 7942 SIP, and 7945 SIP models, which are equivalent, can share an EM profile.
- 7960 SCCP and 7961 SCCP models, which are equivalent, can share an EM profile.
- 7962 SCCP and 7965 SCCP models, which are equivalent, can share an EM profile.
- 7960 SIP, 7961 SIP, 7962 SIP, and 7965 SIP models, which are equivalent, can share an EM profile.
- 7970 SCCP and 7971 SCCP models, which are equivalent, can share an EM profile.
- 7970 SIP, 7971 SIP, and 7975 SIP models, which are equivalent, can share an EM profile.

The enhancement works for all phone models that are equivalent and requires no administration tasks to activate.

Note Be aware that this feature does not support using an EM profile that is configured for a newer model on the Cisco Unified IP Phone 7960 or 7940.

Cisco Unified Communications Manager Administration Configuration Tips

To configure a phone button template for a Cisco Unified IP Phone, choose the **Device > Device Settings > Phone Button Template** in Cisco Unified Communications Manager Administration.

Serviceability Considerations

Cisco Extension Mobility relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Extension Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

User Tips

Refer to the "Description" section on page 48 for this feature.

For More Information

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

Cisco Unified Communications Manager Attendant Console Support in 7.0(2)

If you are upgrading from a compatible Cisco CallManager 4.X release or a compatible Cisco Unified Communications Manager 5.X, 6., or 7.0(x) release to Cisco Unified Communications Manager Release 7.0(2), you can continue to use the Cisco Unified Communications Manager Attendant Console. As automated within the Cisco Unified Communications Manager upgrade process, the Cisco Unified Communications Manager Attendant Console plug-in will remain viewable from the Find and List Plugins window in Cisco Unified Communications Manager Administration 7.0(2).

Be aware, however, that Cisco no longer supports the Cisco Unified Communications Manager Attendant Console with new installations of Cisco Unified Communications Manager 7.0(x). For new installations, the Cisco Unified Communications Manager Attendant Console plug-in does not display in the Find and List Plugins window in Cisco Unified Communications Manager Administration.

If you previously obtained the Cisco Unified Communications Manager Attendant Console 7.0(1) plug-in from the Cisco software download site, you can use that plug-in with Cisco Unified Communications Manager 7.0(x) but only for upgrades of a compatible Cisco Unified Communications Manager 5.X, 6.X, or 7.0(x) release to Cisco Unified Communications Manager Release 7.0(x). Cisco Systems does not authorize the use of the Cisco Unified Communications Manager Attendant Console 7.0(x) plug-in with new Cisco Unified Communications Manager 7.0(x) installations, and its use does not get supported by the Cisco Technical Assistance Center.

If you need attendant console functionality after a Cisco Unified Communications Manager 7.0(x) installation/upgrade, Cisco recommends that you use the Cisco Unified Business Attendant Console, Cisco Unified Enterprise Attendant Console, or the Cisco Unified Department Attendant Console.

For More Information

- Cisco Unified Communications Manager Attendant Console End of Life and End of Sale Announcement—http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7046/ps7282/end_of_life_notice_c51-499091.html
- *Cisco Unified Communications Manager Software Compatibility Matrix* —For information on the versions of Cisco Unified Business Attendant Console, Cisco Unified Enterprise Attendant Console, or Cisco Unified Department Attendant Console that are compatible with Cisco Unified Communications Manager 7.0(x)
- http://www.cisco.com/en/US/products/ps7282/tsd_products_support_series_home.html

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

Cisco Unified IP Phone Expansion Module 7915 and 7916 Support

Cisco Unified Communications Manager 7.0 adds support for the Cisco Unified IP Phone Expansion Module 7915 and Cisco Unified IP Phone Expansion Module 7916. The Cisco Unified IP Phone Expansion Module 7915 and Cisco Unified IP Phone Expansion Module 7916 attach to the following phones:

- Cisco Unified IP Phone 7962G

- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7975G

Each expansion module adds up to 24 extra line appearances or programmable buttons to a phone. You can attach up to two expansion modules to a Cisco Unified IP Phone for a total of 48 extra line appearances or programmable buttons.

Cisco Unified Communications Manager Administration Configuration Tips

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

For More Information

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

Cisco Unified Mobility—Cisco Unified Mobile Communicator

The Cisco Unified Mobile Communicator (CUMC) specifies a device type that you can configure in Cisco Unified Communications Manager Administration in the Phone Configuration window. The Cisco Unified Mobile Communicator operates with the Mobile Smart Client device protocol and uses three Device License Units (DLUs), or one DLU, if adjunct.

Cisco Unified Communications Manager Administration Configuration Tips

The following configuration takes place in Cisco Unified Communications Manager Administration to provision and enable the Cisco Unified Mobile Communicator device:

1. Configure a Cisco Unified Mobile Communicator (CUMC) device. Use the **Device > Phone** menu option.

   Note Make sure that you check the Enable Mobility check box in the End User Configuration window.

   Note Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for Mobile Connect.

2. Configure a security profile for a CUMA server. Use the **System > Security Profile > CUMA Server Security Profile** menu option.
3. Configure an application server for a CUMA server. Use the **System > Application Server** menu option. In the Application Server Type drop-down list box, choose the CUMA Provisioning Server type.
4. Configure the enterprise feature access directory number (DN). Use the **Call Routing > Directory Number** menu option. You must perform this configuration step for the Dial-via-Office features to work.
5. Allow the CUMA client to register with Cisco Unified Communications Manager.

6. Perform the following configuration for end users: configure a CUMC device for a particular end user; configure a remote destination for an end user that specifies the CUMC device as the remote destination profile. Alternately, allow end users to configure these settings for themselves through use of the Cisco Unified CM User Options windows.

Cisco Unified Mobile Communicator Configuration Details

When you configure a Cisco Unified Mobile Communicator (CUMC), keep in mind the following configuration requirements as you configure the fields in the Phone Configuration window:

- When you configure a new Cisco Unified Mobile Communicator, select the phone type Cisco Unified Mobile Communicator in the Select Phone Type drop-down list box.
- Device Name—Ensure this name is unique. You need no MAC address.
- Mobility User ID—You must configure this field.
- Mobility Identity—This field must specify the CUMC-enabled smartphone mobile number as the destination number.
- Reroute CSS, CSS—Ensure these fields are configured for basic calls to work.
- DND Option—The Cisco Unified Mobile Communicator only supports the Call Reject DND option.

Ensure that a directory number is assigned to the Cisco Unified Mobile Communicator.

Keep in mind these other configuration requirements that apply to the Cisco Unified Mobile Communicator:

- Due to the lack of an integrated End User Configuration window for Cisco Unified Communications Manager and the Cisco Unified Mobility Advantage server, the CUMC client user must configure identical remote destination numbers in both Cisco Unified Communications Manager Administration and in the Cisco Unified Mobility Advantage server.
- Refer to the "AXL and CTI Considerations" section on page 53 for an AXL consideration that you must take into account when a CUMC client user changes the user SIM card.
- The Cisco Unified Mobility Advantage server only uses AXL to update the Cisco Unified Communications Manager database but ignores the Cisco Unified Communications Manager database change notifications.

Cisco Unified Mobile Communicator General Considerations

Keep in mind the following general considerations for the Cisco Unified Mobile Communicator device:

- You can add one or more remote destinations to the CUMC device (similar to the remote destination profile).
- No automatic migration support exists. You must manually reconfigure the device as a CUMC device.
- Only the first call gets supported because, in 2.5G, the data channel does not remain available after the voice call connects.
- The CUMA server can activate only one CUMC device per user.
- In configuration of the CUMC device, the reroute CSS and CSS represent key considerations.

GUI Changes

This feature entails the following GUI changes in Cisco Unified Communications Manager Administration:

- The new menu option **System > Security Profile > CUMA Server Security Profile** allows configuration of a security profile for the CUMA server.
- The **System > Application Server** menu option allows configuration of a new application server type, CUMA Provisioning Server.
- The **Device > Phone** menu option allows configuration of a new phone type, Cisco Unified Mobile Communicator.
- The **Device > Remote Destination** menu option adds a new setting, Cisco Unified Mobile Communicator.

Service Parameter and Enterprise Parameter Changes

This feature entails no service or parameter changes in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

No installation considerations exist for this feature.

No automatic migration support exists for remote destinations. For a remote destination to be upgraded to a Cisco Unified Mobile Communicator device, manual upgrade of the remote destination must occur.

Serviceability Considerations

Cisco Unified Mobility relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Unified Mobile Voice Access service, which allows mobile voice access to function. Before you configure this feature, activate the Cisco Unified Mobile Voice Access service in Cisco Unified Serviceability.

Security Considerations

Configure the security profile for the CUMA server by using the **System > Security Profile > CUMA Server Security Profile** menu option in Cisco Unified Communications Manager Administration.

AXL and CTI Considerations

The following AXL consideration exists for this feature:

- If a Cisco Unified Mobile Communicator (CUMC) client user ever changes the user SIM card, the user must update the mobile number on the CUMC server. The CUMC server then uses AXL with the old mobile number to update Cisco Unified Communications Manager with the new mobile number and sends a new SIP REGISTER message to Cisco Unified Communications Manager.

No CTI considerations exist for this feature.

User Tips

Users can configure their own Cisco Unified Mobile Communicator devices by using the Cisco Unified CM User Options windows. Users can specify the following settings:

- Device—End user specifies his own Cisco Unified Mobile Communicator.
- Remote Destinations—End user chooses his own Cisco Unified Mobile Communicator as the remote destination profile.

For More Information

- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Call Park and Directed Call Park," *Cisco Unified Communications Manager Features and Services Guide*
- "Configuring a CUMA Server Security Profile," *Cisco Unified Communications Manager Security Guide*
- "Application Server Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Time Period Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Time Schedule Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "End User Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Licensing," *Cisco Unified Communications Manager System Guide*
- "Application Users and End Users," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Mobility—Dial-via-Office Reverse Callback

The Cisco Unified Mobility Dial-via-Office Reverse Callback feature resembles the Mobile Voice Access feature, except that Cisco Unified Communications Manager makes both calls. From the Cisco Unified Mobile Communicator (CUMC) client, using the data channel, the phone initiates the Reverse Callback feature. Cisco Unified Communications Manager then calls the remote destination first. When the remote destination answers, Cisco Unified Communications Manager calls the destination number.

Example of Dial-via-Office Reverse Callback

The following example illustrates the sequence of events that takes place in an instance of dial-via-office reverse callback:

1. User invokes the dial via office feature on the phone and calls target DN 2000.
2. Phone sends INVITE 2000 with the callback number that is specified in the SDP parameter c=PSTN E164 4085551234.
3. Cisco Unified Communications Manager sends back 183 Session In Progress with Enterprise Feature Access Number (4085556666) in SDP parameter.
4. Cisco Unified Communications Manager calls back remote destination 4085551234.
5. When the remote destination answers the call, Cisco Unified Communications Manager redirects the call to the target DN 2000.

Example of Dial-via-Office Reverse Callback to Remote Phone

Using the preceding example, the following characteristics apply to a Reverse Callback instance when a remote phone is called:

1. Based on SDP parameter a=setup:passive, Cisco Unified Communications Manager determines its dial-via-office (reverse) call.
2. Cisco Unified Communications Manager sends a SIP/2.0 183 Session Progress message.
3. Based on SDP parameter c=PSTN E164 4085551234, Cisco Unified Communications Manager calls back remote phone.
4. Remote phone answers and gets redirected to the target DN 2000.

CUMA support for this feature exists.

Example of Dial-via-Office Reverse Callback to Non-Remote Phone

Using the preceding example, the following characteristics apply to a Reverse Callback instance when a non-remote phone is called:

1. Based on SDP parameter "a=setup:passive," Cisco Unified Communications Manager determines its dial-via-office (reverse) call.
2. Cisco Unified Communications Manager sends "SIP/2.0 183 Session Progress" message.
3. Based on SDP parameter "c=PSTN E164 4085553456," Cisco Unified Communications Manager calls back the non-remote phone, which can represent any PSTN phone at which the user wants to be contacted. A hotel phone.represents an example of such a phone.
4. Non-Remote Phone (4085553456) answers and gets redirected to the target DN 2000.

CUMA support for this feature exists.

Cisco Unified Communications Manager Administration Configuration Tips

The administrator must configure the enterprise feature access directory number (DN). Use the **Call Routing > Directory Number** menu option. You must perform this configuration step for the Dial-via-Office features to work.

GUI Changes

This feature entails no changes to the Cisco Unified Communications Manager Administration GUI.

Service Parameter and Enterprise Parameter Changes

This feature entails no service or enterprise parameter changes in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

No installation considerations exist for this feature.

No automatic migration support exists for remote destinations. For a remote destination to be upgraded to a Cisco Unified Mobile Communicator device, manual upgrade of the remote destination must occur.

Serviceability Considerations

Cisco Unified Mobility relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Unified Mobile Voice Access service, which allows mobile voice access to function. Before you configure this feature, activate the Cisco Unified Mobile Voice Access service in Cisco Unified Serviceability.

AXL and CTI Considerations

The following AXL consideration exists for this feature:

- If a Cisco Unified Mobile Communicator (CUMC) client user ever changes the user SIM card, the user must update the mobile number on the CUMC server. The CUMC server then uses AXL with the old mobile number to update Cisco Unified Communications Manager with the new mobile number and sends a new SIP REGISTER message to Cisco Unified Communications Manager.

No CTI considerations exist for this feature.

User Tips

This feature functions only for remote destinations that have configured a Cisco Unified Mobile Communicator client.

For More Information

- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "End User Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Application Users and End Users," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Mobility—Directed Call Park via DTMF

A user can park an existing call by using DTMF digits. Using Directed Call Park from the mobile phone, a user parks a call and inputs a unique mobility user park code. The user can subsequently retrieve the call with the code or have someone else retrieve the call with the code. This feature proves useful for certain vertical markets that require different departments or users to pick up calls.

When a user is in the enterprise and picks up a call on their mobile phone, they may want to pick the call up on a Cisco Unified IP Phone in a conference room or desk where the DN is not visible. The user can park the call and pick up the parked call with only their code.

When the mobile phone user is on an active call, by using the DTMF transfer feature, the user can park the call by transferring the parkee party to the park code that the system administrator configures and assigns to the user.

This feature allows the mobile phone user to park a call by transferring the parkee party to a user-selected park code. When the mobile phone user is on an active call, by using the DTMF transfer feature, the user can park the call by transferring the parkee party to the user-selected park code. The dialing sequence resembles the DTMF transfer sequence, except that a preconfigured parking code replaces the transfer number.

Example of Directed Call Park via DTMF—Parking the Call

In the following example, *82 specifies exclude hold, *84 specifies transfer, the pin specifies 12345, and the call park code specifies 3215. The following actions take place from the mobile phone:

1. Dial *82 (to put the call on enterprise hold).
2. If necessary, put the mobile phone call on Hold, depending on the mobile phone model.
3. Make a new call to the enterprise with feature DID.
4. After the call connects, dial this digit sequence: 12345#*84#3215#*84#.

Cisco Unified Communications Manager puts the parkee party on hold and provides dial tone to the parker party, just like the Call Transfer feature.

After Cisco Unified Communications Manager receives the dialed park code digit, the digit analysis engine verifies whether the dialed park code digits are valid. If so, the Directed Call Park feature intercepts the park code and verifies whether the park code is available. If the dialed park code is valid and available, the parker party receives the ringback tone, and the secondary call terminates to a Cisco Unified Communications Manager generic device that associates with the selected park code. The generic device automatically answers and places the parker party on hold with music on hold (MOH) or tone on hold. The last *84 completes the transfer of the parkee to the Cisco Unified Communications Manager generic device that associates with the selected park code. After the transfer completes, the parkee party receives the MOH or tone on hold, and the parkee gets parked on this selected park code and waits for retrieval.

If another user is already using the user-selected park code, Directed Call Park feature logic in Cisco Unified Communications Manager rejects that selected park code and plays busy tone to the parker party. The user gets to select another park code.

If the user-selected park code is not valid, Cisco Unified Communications Manager plays reorder tone to the parker party, and the user gets to select another park code.

For the Directed Call Park feature, be aware that the park code and code range are configurable throughout the system. Every Cisco Unified Communications Manager server in the system shares the park code and code range.

Example of Directed Call Park via DTMF—Retrieving the Parked Call

When a user attempts to retrieve the parked call, the user can go off hook on another mobile phone, and the user must use two-stage dialing to dial a digit string that contains the Directed Call Park retrieval prefix digits (for example, 22) plus the park code/code range (for example, 3215). The following sequence of events takes place:

1. Dial Enterprise Feature DID on mobile phone.
2. Upon connection, press PIN#1#223215 to retrieve the parked call.

Just like the existing Call Park feature, if the call does not get retrieved on time, the parked call reverts, by default, to the phone number that is associated with the parker party.

If a shared line is configured for the phone line of the parker, all phones that are associated with the shared line will ring. In addition, the dPark feature allows the user to configure a call park reversion number in the Call Park Administration window, so, if the call park reversion number is configured, the non-retrieved call reverts to this number, instead of to the parker party number.

Cisco Unified Communications Manager Administration Configuration Tips

If users want to park calls on extension numbers, the administrator needs to configure a park code or park code range that has extension numbers that compose part of the park code or park code range. For example, if the Cisco Unified Communications Manager system has extension DN range as 3xxx, the administrator can configure a park code range of 213xxx. When a user who has extension 3555 wants to

park call on a park code that is associated with his extension, the user can dial park code 213555. Otherwise, call processing will not know whether the user attempts to transfer the call to an extension number or to park the call on a park code that is associated with an extension number.

When a user attempts to retrieve the parked call, the user can go off hook on another mobile phone, and the user must dial a digit string that contains directed call park retrieval prefix digits plus the park code/code range.

If directed call park park codes or code ranges overlap, or park codes/code ranges overlap with a DN range, the user may experience delay to retrieve a parked call due to interdigit time out. This represents an existing limitation of Cisco Unified Communications Manager. To avoid delays in retrieving a parked call, do not configure overlapped park codes/code ranges and do not overlap park codes/code ranges with the extension DN range.

Just like the existing call park feature, if a call is parked by the directed call park feature logic and the call is not retrieved on time, the parked call reverts to the address that is associated with the parker party by default. If a shared line is configured for the phone line of the parker, all phones that are associated with the shared line will ring. In addition, the directed call park feature allows the user to configure a call park reversion number in the Directed Call Park Configuration window, so, if the call park reversion number is configured, the nonretrieved call will revert to this number instead of to the party number of the parker.

GUI Changes

This feature entails no changes to the Cisco Unified Communications Manager Administration GUI.

Service Parameter and Enterprise Parameter Changes

This feature entails no service or enterprise parameter changes in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

This feature does not require installation in Cisco Unified Communications Manager Administration.

This feature entails no upgrade (migration) considerations in Cisco Unified Communications Manager Administration.

Serviceability Considerations

Cisco Unified Mobility relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Unified Mobile Voice Access service, which allows mobile voice access to function. Before you configure this feature, activate the Cisco Unified Mobile Voice Access service in Cisco Unified Serviceability.

User Tips

The “Cisco Unified Mobility” chapter of the *Cisco Unified Communications Manager Features and Services Guide* provides examples of use cases for the Cisco Unified Mobility Directed Call Park with DTMF feature.

For More Information

Refer to the following documents for additional configuration details for this feature:

- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Call Park and Directed Call Park," *Cisco Unified Communications Manager Features and Services Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "End User Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Mobility—SIP URI Dialing

Description

This feature supports Session Initiation Protocol (SIP) Universal Resource Identifier (URI) as an additional type of remote destination for Cisco Unified Mobility. When the DN is called, Cisco Unified Communications Manager extends the call to a SIP trunk that digit analysis selects with this SIP URI in the To: header.

This feature only allows routing that is based only on the domain name, not based on the full SIP URI.

When a remote destination of this type is configured, other Cisco Unified Mobility features, such as two-stage dialing, transformation to DN number when calling into Cisco Unified Communications Manager, Interactive Voice Response (IVR) support, caller ID match, or DTMF transfer and conferencing, do not get supported.

SIP URI Example

For a remote destination, the SIP URI *user@corporation.com* is configured. Be aware that a SIP route pattern that specifies *corporation.com* must also be configured for the SIP URI remote destination to resolve correctly.

Cisco Unified Communications Manager Administration Configuration Tips

The SIP URI dialing feature entails a relaxation of the business rules to allow the entry of a URI in the Destination Number field of the Remote Destination Configuration window. (From Cisco Unified Communications Manager Administration, choose the **Device > Remote Destination** menu option.)

An additional requirement for this feature specifies that a SIP route pattern that matches the configured URI domain must be configured for the feature to work. To configure a SIP route pattern, from Cisco Unified Communications Manager Administration, choose the **Call Routing > SIP Route Pattern** menu option.

GUI Changes

This feature entails no changes to the Cisco Unified Communications Manager Administration GUI, but the Destination Number field of the Remote Destination Configuration window now allows entry of a SIP URI.

Service Parameter and Enterprise Parameter Changes

This feature entails no service or enterprise parameter changes in Cisco Unified Communications Manager Administration.

Serviceability Considerations

Cisco Unified Mobility relies on the Cisco CallManager service, so before you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Unified Mobile Voice Access service, which allows mobile voice access to function. Before you configure this feature, activate the Cisco Unified Mobile Voice Access service in Cisco Unified Serviceability.

AXL and CTI Considerations

The following AXL consideration exists for this feature:

- If a Cisco Unified Mobile Communicator (CUMC) client user ever changes the user SIM card, the user must update the mobile number on the CUMC server. The CUMC server then uses AXL with the old mobile number to update Cisco Unified Communications Manager with the new mobile number and sends a new SIP REGISTER message to Cisco Unified Communications Manager.

No CTI considerations exist for this feature.

User Tips

See the "Description" section on page 59 for a description of the features that the user can access upon receiving a call to a SIP URI.

For More Information

- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Application Server Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "End User Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Application Users and End Users," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*

Cisco Unified Mobility—Time-of-Day (ToD) Access

An access list determines whether a call should be extended to a remote destination that is enabled for the Mobile Connect feature. With the addition of time-based control, the Time-of-Day Access feature adds time as another determination factor. The feature allows administrators and users to determine whether a call should reach a remote destination based on the time of day when the call is received.

For calls to remote destinations, the Time-of-Day Access feature adds a ring schedule and associates the ring schedule with an access list to determine the time-of-day access settings for a remote destination.

The provisioning process includes provisioning the following entities:

- Access lists
- Remote destinations (configuring a ring schedule and associating the ring schedule with an access list for a remote destination)

As an extension to the existing access list feature, ensure the Time-of-Day Access feature is accessible to end users of Cisco Unified Communications Manager. Therefore, you can provision the feature through use of both Cisco Unified Communications Manager Administration (by administrators) and Cisco Unified CM User Options (by end users).

Time-of-Day Access Example

The following example illustrates a specific time-of-day access application:

Block 1800! during business hours for user browser.

Cisco Unified Communications Manager Administration Configuration Tips

The following procedure provides an overview of the configuration that administrators perform in Cisco Unified Communications Manager Administration to configure the Time-of-Day Access feature for Cisco Unified Mobility:

1. In Cisco Unified Communications Manager Administration, configure an end user for whom you will enable the Time-of-Day Access feature.

   Use the **User Management > End User** menu option.

   Note Make sure that you check the Enable Mobility check box in the End User Configuration window.

   Note Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for mobile connect.

2. For a particular user, configure access lists to use for time-of-day access by assigning each list to the user. Create separate access lists for callers that are allowed and callers that are blocked.

   Note Ensure an access list has an owner. No system access list exists.

   Use the **Call Routing > Class of Control > Access List** menu option.

3. Configure a remote destination for a user. Remote destinations represent the mobile (or other) phones that can accept transfers from the user desktop phone and that can initiate calls by using mobile voice access.

   Use the **Device > Remote Destination** menu option.

   Note The same configuration also applies to dual-mode phones and to Cisco Unified Mobile Communicator Mobility Identity to set up time-of-day access.

   For successful time-of-day access configuration, you must configure the following areas in the Remote Destination Configuration window:

   - Use the Ring Schedule pane to configure a ring schedule for the remote destination.
   - Use the *When receiving a call during the above ring schedule* pane to specify the access list for which the ring schedule applies.

Checking the Enable Mobile Connect check box for the remote destination enables Cisco Unified Mobility to apply the settings in the When Mobile Connect is Enabled pane to calls that are made to this remote destination. If the Enable Mobile Connect check box is not checked, the settings do not apply to incoming calls to this remote destination, but the settings remain intact for future use.

Important Notes for Time-of-Day Access

The following important notes apply to time-of-day access configuration:

- A ring schedule associates with the time zone of a remote destination, not with the time zone of the Cisco Unified Communications Manager server. Use the Time Zone field in the Remote Destination Configuration window to specify the time zone of the remote destination.
- If a remote destination has no time-of-day access configuration, all calls get extended to the remote destination. By default, the All the time ring schedule radio button and the Always ring this destination radio button are checked, so all calls get extended to the remote destination.
- Cisco recommends that you always configure an access list with members; avoid creating an empty access list that contains no members. If an empty access list is chosen in the *Ring this destination only if the caller is in* drop-down list box, all calls get blocked (instead of allowed). If an empty access list is chosen in the *Do not ring this destination if the caller is in* drop-down list box, all calls get allowed during the specified ring schedule. Either use of an empty access list could cause unnecessary confusion for end users.

Refer to the user guide for the applicable Cisco Unified IP Phone model for details of the settings that end users can configure to customize their time-of-day access settings by using the Cisco Unified CM User Options windows.

GUI Changes

The following changes occurred to Cisco Unified Communications Manager Administration menu items:

- **Device > Remote Destination**—Changes to the Remote Destination Configuration window
- **Device > Device Settings > Remote Destination Profile**—Changes to the Remote Destination Profile Configuration window
- **Call Routing > Class of Control > Access List**—This menu item displayed in the **Device > Device Settings** menu in earlier releases of Cisco Unified Communications Manager.

Service Parameter and Enterprise Parameter Changes

This feature entails no service or enterprise parameter changes in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

This feature does not require installation in Cisco Unified Communications Manager Administration.

The following database upgrade (migration) considerations exist for this feature during an upgrade from an earlier release to Release 7.0(of Cisco Unified Communications Manager:

- During database installation, Cisco Unified Communications Manager populates a TimeSchedule row (and corresponding TimePeriod rows) to automatically create a continuous time schedule without start or end date (called anytime-schedule). Ensure this time schedule has isPublished set to 't'.

- Cisco Unified Communications Manager migrates all the activated access lists that are provisioned in Release 6.0(x). Cisco Unified Communications Manager automatically creates ToDAccess and ToDAccessSetting records for each activated access list to associate this access list with a system-created continuous time schedule. Cisco Unified Communications Manager also associates such a ToDAccess record with the remote destination on which the access list is activated.
- Cisco Unified Communications Manager migrates the Smart Client Installed field to the new tkClientAppModel = CLIENT_APP_MODEL_ STANDARD.

Refer to the "Supported Use Cases for Migrating Activated Access Lists from an Earlier Cisco Unified Communications Manager Release" section on page 64 for details of migration considerations for activated access lists that were created in an earlier release of Cisco Unified Communications Manager.

Serviceability Considerations

Cisco Unified Mobility relies on the Cisco CallManager service, sobefore you configure this feature, activate the service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Extension Mobility service, which allows users to log in or log out of phones via Cisco Extension Mobility. Before you configure this feature, activate the Cisco Extension Mobility service in Cisco Unified Serviceability.

Cisco Unified Mobility relies on the Cisco Unified Mobile Voice Access service, which allows mobile voice access to function. Before you configure this feature, activate the Cisco Unified Mobile Voice Access service in Cisco Unified Serviceability.

BAT Considerations

In anticipation of new Cisco Unified Mobility features, Release 7.0 of Cisco Unified Communications Manager must support bulk provisioning of time periods, time schedules, and time-of-day access records through use of the Bulk Administration Tool (BAT).

In earlier releases, the Bulk Administration Tool provided manual migration support for MobilityManager 1.2.x to Release 7.0 of Cisco Unified Communications Manager.

The import/export function of the Bulk Administration Tool provides bulk insert and export support for time periods and time schedules. BAT and MobilityManager (for migration) user documentation provides details for how to bulk provision time-of-day access records (including where to insert time periods and time schedules).

Cisco Unified Communications Manager Bulk Administration Tool adds the following new submenu items to add/modify/delete/export time of day access settings:

- Bulk Administration > Mobility > Time of Day Access > Insert Time of Day Access
- Bulk Administration > Mobility > Time of Day Access > Delete Time of Day Access
- Bulk Administration > Mobility > Time of Day Access > Export Time of Day Access

The Cisco Unified Communications Manager Bulk Administration Tool **Bulk Administration > Mobility** submenu specifies all the mobility-related menu items (Access List, Remote Destination, Remote Destination Profile, Time of Day Access) to provide a tightly coupled navigation experience.

User Tips

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* provides examples of use cases.

The use case scenarios that follow detail the function of the time-of-day access feature with activated access lists that were configured prior to the addition of the time-of-day access feature in Release 7.0 of Cisco Unified Communications Manager, as well as with new provisioning that takes place for the feature starting with Release 7.0 of Cisco Unified Communications Manager.

Supported Use Cases for Migrating Activated Access Lists from an Earlier Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility when migration of an activated access list from a, earlier release of Cisco Unified Communications Manager to Release 7.0(x) or later takes place:

- Use Case #1—No allowed or blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: The system allows all calls at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button gets checked. In the When Receiving a call during the above ring schedule pane, the Always ring this destination radio button gets checked.

- Use Case #2—Only an allowed access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: Only the callers that belong to the allowed access list can reach the associated remote destination. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button displays as checked. In the When Receiving a call during the above ring schedule pane, the Ring this destination only if caller is in radio button displays as checked, and the access list displays in the corresponding drop-down list box.

- Use Case #3—Only a blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.

  Result after migration: The callers that belong to the blocked access list cannot reach the associated remote destination, but all other callers can call the remote destination at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button displays as checked. In the When Receiving a call during the above ring schedule pane, the Do not ring this destination if caller is in radio button displays as checked, and the access list displays in the corresponding drop-down list box.

Use Cases for Time-of-Day Access with the Current Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility with the 7.0 release of Cisco Unified Communications Manager:

- Use Case #4—Only allow calls during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday and click the Always ring this destination radio button.

  Result: The system allows all callers during business hours, but no calls get extended to this remote destination outside of business hours.

- Use Case #5—Only allow calls from certain numbers (for example, from coworkers) during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, click the Ring this destination only if the caller is in radio button, and specify an access list.

  Result: Only callers that belong to the access list can call the remote destination during business hours; all other callers get blocked during business hours. Outside business hours, no calls ring this remote destination.

- Use Case #6—Block certain numbers (for example, 1800 numbers) during business hours.

  Configuration: Configure a ring schedule that specifies business hours from Monday to Friday, click the Don’t ring this destination if the caller is in radio button, and specify an access list.

Result: Only callers that belong to the access list get blocked from calling the remote destination during business hours; all other callers can call the remote destination during business hours. Outside business hours, no calls ring this remote destination.

For More Information

Refer to the following documents for additional configuration details for this feature:

- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Time Period Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Time Schedule Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "End User Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Licensing," *Cisco Unified Communications Manager System Guide*
- "Application Users and End Users," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- Cisco Unified Mobility Chapter Omits Information about the DN Mask Field, page 173

Cisco Click-to-Conference Plug-In with IBM SameTime

For information on this feature, refer to the *Integration Guide for Configuring the Cisco Click-to-Conference Plug-In with IBM Lotus Sametime*, which describes how to configure Cisco Unified Communications Manager for this feature. To locate this document, go to http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_configuration_examples_list.html.

Before you configure this feature, refer to the *Cisco Unified Communications Manager Software Compatibility Matrix* for the click-to-conference feature at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.

Directed Call Pickup

The Directed Call Pickup feature allows a user to pick up a ringing call on a directory number (DN) directly by pressing the GPickUp softkey and entering the directory number of the device that is ringing. Cisco Unified Communications Manager uses the associated group mechanism to control the privilege of a user who wants to pick up an incoming call by using Directed Call Pickup. The associated group of a user specifies one or more call pickup groups that have been associated to the pickup group to which the user belongs.

Cisco Unified Communications Manager Administration Configuration Tips

If a user wants to pick up a ringing call from a DN directly, the associated groups of the user must contain the pickup group to which the DN belongs. If two users belong to two different call pickup groups and the associated groups of the users do not contain the call pickup group of the other user, the users cannot invoke Directed Call Pickup to pick up calls from each other.

If a user wants to pick up a ringing call from a DN directly, the associated groups of the user must contain the pickup group to which the DN belongs. If two users belong to two different call pickup groups and the associated groups of the users do not contain the call pickup group of the other user, the users cannot invoke Directed Call Pickup to pick up calls from each other.

When the user invokes the Directed Call Pickup feature and enters a DN from which to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest ringing call in the call pickup group to which the DN belongs.

If multiple calls are ringing on a particular DN and the user invokes Directed Call Pickup to pick up a call from the DN, the user connects to the incoming call that has been ringing the specified DN the longest.

GUI Changes

This feature entails no changes to the Cisco Unified Communications Manager Administration GUI.

Service Parameter and Enterprise Parameter Changes

This feature does not require any changes to the existing service or existing enterprise parameters in Cisco Unified Communications Manager Administration.

CAR/CDR Considerations

No CAR considerations exist for this feature.

The following CDR consideration exists for this feature:

- The onBehalfOf value specifies (Pickup) 16, which represents the Call Pickup feature. This value gets used when a Call Pickup is taking place. The redirectOnBehalfOf and joinOnBehalfOf fields for the Directed Pickup CDRs get set to (Pickup) 16. Both of these fields contain the same value. The original called party number stays the same for both auto and non-auto pickup.

User Tips

Be aware that the following restrictions are imposed upon users who try to use the Directed Call Pickup feature:

- Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.
- If a device belongs to a hunt list and the device rings due to a call that was made by calling the hunt pilot number, users cannot use the Directed Call Pickup feature to pick up such a call.

These restrictions apply beyond the configuration requirements that are detailed in the "Cisco Unified Communications Manager Administration Configuration Tips" section on page 65.

For More Information

- "Call Pickup," *Cisco Unified Communications Manager Features and Services Guide*
- "Call Pickup Group Configuration," Cisco Unified Communications Manager Administration
- "System Configuration Overview," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- "Directory Number Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Multilevel Precedence and Preemption," *Cisco Unified Communications Manager Features and Services Guide*
- "Line Group Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Hunt List Configuration," *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* (all models)
- Cisco Unified IP Phone user documentation and release notes (all models)

Do Not Disturb Call Reject

The Do Not Disturb (DND) Call Reject feature, which is an enhancement to Do Not Disturb, allows the user or the administrator to configure Cisco Unified Communications Manager, so no incoming call information gets presented to user.

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

The user can enable and disable DND by any of the following methods:

- Softkey
- Feature Line Key
- Cisco Unified CM User Options windows

The system administrator can also enable and disable DND on a per-phone basis in Cisco Unified Communications Manager Administration.

When you enable DND, the Cisco Unified IP Phone displays the message that Do Not Disturb is active. The DND line button icon also turns into an empty circle, and the light turns amber when DND is active.

Cisco Unified Communications Manager Administration Configuration Tips

When you enable DND on a device, the DND Option parameter allows you to specify how the DND features handle incoming calls:

- **Call Reject**—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.
- **Ringer Off**—This option turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.
- **Use Common Phone Profile Setting**—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device.

Note The Use Common Phone Profile Setting parameter does not display on the Common Phone Profile Configuration window.

When you choose the DND Ringer Off or Call Reject option, DND Incoming Call Alert parameter specifies how a call displays on a phone.

- **None**—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device.
- **Disable**—This option disables both beep and flash notification of a call, but, for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display, and no information gets sent to the device.
- **Beep Only**—For an incoming call, this option causes the phone to play a beep tone only.
- **Flash Only**—For an incoming call, this option causes the phone to display a flash alert.

Note For Cisco Unified IP Phones 7940/7960 that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

GUI Changes

To support DND Call Reject, Cisco Unified Communications Manager now includes the DND Option parameter.

To access the DND Option parameter for phones, choose **Device > Phone**.

To configure a device profile with DND Call Reject, choose **Device > Device Settings > Device Profile**.

To set up a common phone profile with DND Call Reject, choose **Device > Device Settings > Common Phone Profile**.

To configure a Remote Destination Profile with DND Call Reject, choose **Device > Device Settings > Remote Destination Profile.**

For More Information

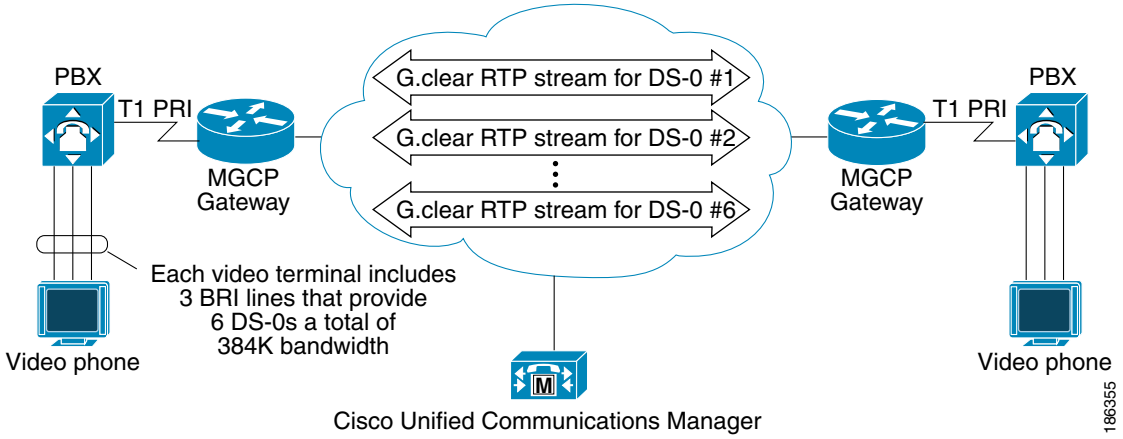
- "Do Not Disturb," *Cisco Unified Communications Manager Features and Services Guide*
- "Common Phone Profile Configuration," Cisco Unified Communications Manager Administration
- "Device Profile Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*
- "Cisco Unified Mobility," *Cisco Unified Communications Manager Features and Services Guide*

G.Clear Codec Support

The G. Clear (Clear channel) codec enables tandem switching of Digital Signal-0 (DS-0) data circuits through a voice network that uses Media Gateway Control Protocol (MGCP) gateways, Session Initiation Protocol (SIP) trunks, and Cisco Unified Communications Manager. The MGCP gateway uses T1 PRI DS-0 circuits to communicate with Cisco Unified Communications Manager.

Figure 1 shows an example of the G.Clear codec configuration in an MGCP network. In this example, legacy video terminals, such as Polycoms, connect to separate PBX switches that are interconnected by the MGCP gateway. The terminals set up individual calls for each DS-0 by using "unrestricted digital information" in the Q.931 bearer capability. Cisco Unified Communications Manager treats the incoming ISDN signal as a voice call that is using G.Clear.

Figure 1 MGCP Network with G.Clear Codec



The G.Clear codec uses 64 kb/s of bandwidth (not including IP packet overhead), which is similar to the G.711 codec. The Cisco Unified Communications Manager Region Manager selects the codec of a voice call and prioritizes the G. Clear codec ahead of the G.711 mulaw and G.711 alaw codecs in the Region Manager media table.

You may require the G.Clear codec or the G.729 codec in a region or some other low-bandwidth codec for calls to remote regions. The G.729 codec, which is optimized for speech, uses significantly less bandwidth than the G. Clear codec. Be aware that the G.Clear codec is an option only to explicitly allow it to run in lower bandwidth regions.

G. Clear codec calls require separate DiffServ CodePoint (DSCP) values in the header of IP packets. This differs from traditional voice codecs and video calls and must be tagged uniquely by the MLPP precedence level. Added service parameters apply these capabilities. See the Service Parameter and Enterprise Parameter Changes for more information.

G. Clear codec calls maintain consistency throughout the gateway by using the RTP dynamic payload type 125. The dynamic payload type gets statically allocated by using Cisco Unified Communications Manager.

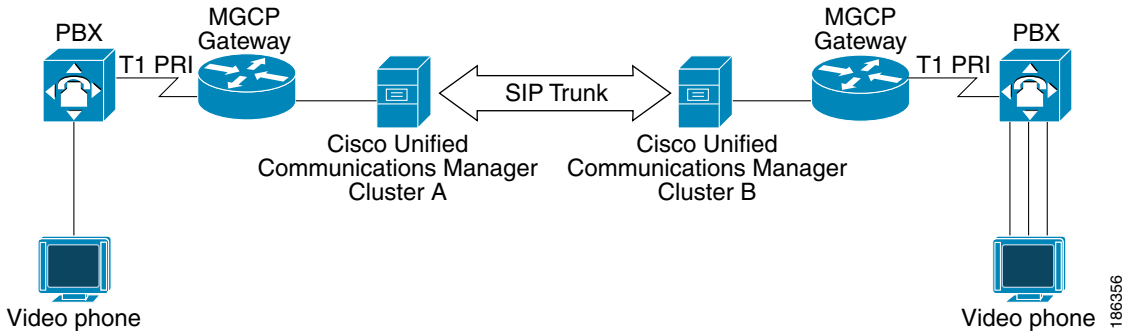
SIP trunk support for the G. Clear codec provides interclusteroperability. The codec, which is negotiated as a supported media type in SIP Session Description Protocol (SDP) messaging, gets statically encoded to RTP payload type 125.

Note No G. Clear codec support exists for media termination points.

Support exists for ISDN bearer capability for incoming ISDN data calls (restricted and unrestricted digital) that exit the VoIP network on another T1 PRI trunk.

Figure 2 shows a typical SIP trunk deployment that has the G.Clear codec enabled.

Figure 2 SIP Trunk Deployment with G. Clear Codec



The following SIP service parameters enable the G. Clear codec over SIP trunks: SIP Route Class Naming Authority and SIP Clear Channel Data Route Class Label. The SIP Route Class Naming Authority parameter represents the naming authority and context for the labels that are used in SIP signaling that represent the route class. The value specifies a domain name that is owned by the naming authority. The default specifies cisco.com.

To signal a particular route class value, Cisco Unified Communications Manager incorporates the domain name and the appropriate route class label, as defined in the SIP Clear Channel Data Route Class Label service parameter, into the SIP signaling.

The SIP Clear Channel Data Route Class Label represents the clear channel data route class in SIP signaling. This parameter and the SIP Route Class Naming Authority parameter create the complete signaling syntax for the SIP clear channel data route class value. The default specifies ccdata.

Route class signaling proves useful when you are interworking with TDM networks that make routing decisions based on route class and clear-channel data route classes. The default domain name that is specified in the parameter applies to interaction between Cisco switches. You can change the parameter to any vendor– or deployment–specific requirements. The far-end switch should receive the same value that is configured in the parameter.

For specific configuration information, see Service Parameter and Enterprise Parameter Changes.

The following entities do not get supported or are disabled:

- ICTs with the G. Clear codec do not get supported.
- Skinny Client Control Protocol (SCCP) devices with the G. Clear codec do not get supported.
- T1 and E1 CAS with the G. Clear codec do not get supported.
- RSVP with the G. Clear codec does not get supported.
- MLPP over E1 trunks does not get supported.
- Echo cancellation and zero suppression for outbound G. Clear codec calls get disabled.
- Frame aligning individual DS-0 circuits that transit the VoIP network do not get supported because terminal equipment takes responsibility for the bonding of the individual DS-0 circuits that are defined by ITU H.244.
- Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work with G. Clear that is enabled.

Cisco Unified Communications Manager Administration Configuration Tips

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

GUI Changes

A check box in the Gateway Configuration window of Cisco Unified Communications Manager Administration enables or disables G. Clear codec functionality. The default sets the check box to disable (no check mark in the box). In Cisco Unified Communications Manager Administration, choose **Device > Gateway**.

Note You must enable the G. Clear Bandwidth Override if you have low-bandwidth codec regions, such as G.711 or G.729. See Service Parameter and Enterprise Parameter Changes for more information.

Service Parameter and Enterprise Parameter Changes

The following service parameters exist for Differentiated Services Code Point (DSCP) values for Quality of Service (QoS) and for overriding bandwidth for G. Clear calls.

Tip To access the following DSCP service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters > Server**. Choose your server from a drop-down list box and Cisco CallManager as the service. Locate the Clusterwide Parameters (Sysem–QoS) pane and choose the appropriate DSCP parameters. To display help for the service parameter, click the link for the service parameter in the Service Parameter Configuration window.

- DSCP for G.Clear Calls
- DSCP for Priority G.Clear Calls (represents the specific MLPP value EF DSCP [101101])
- DSCP for Immediate G.Clear Calls (represents the specific MLPP value EF DSCP [101100])
- DSCP for Flash G.Clear Calls (represents the specific MLPP value EF DSCP [101001])
- DSCP for Flash Override G.Clear Calls (represents the specific MLPP value EF DSCP [101010])
- DSCP for Executive Override G.Clear Calls (represents the specific MLPP value EF DSCP [101010])

Note The Priority, Immediate, Flash, Flash Override, and Executive Override values correspond to discrete MLPP values.

Many DSCP options display for the service parameters; for example, AF11 DSCP (001010), AF12 DSCP (001100), and AF13 DSCP (001110).

Tip To access the G. Clear Bandwidth Override service parameter in Cisco Unified Communications Manager Administration, choose **System > Service Parameters > Server**. Choose your server from a drop-down list box and Cisco CallManager as the service. Locate the Clusterwide Parameters (System–Location and Region) section and choose True. The default specifies False or no override for this required field. To display help for the service parameter, click the link for the service parameter in the Service Parameter Configuration window.

To configure the service parameters for SIP Route Class Naming Authority and SIP Clear Channel Data Route Class Label, choose **System > Service Parameter**. From the drop-down list, choose your server. From the service list, choose **Cisco CallManager**. To display all service parameters, click **Advanced**. Scroll down to the Clusterwide Parameters (Route Class Signaling). Change the SIP Route Class Naming

Authority to the local naming authority and leave the SIP Clear Channel Data Route Class Label parameters set to the default. The following rules apply to both the SIP Route Class Naming Authority and SIP Clear Channel Data Route Class Label parameters:

- Maximum of 64 characters.
- Use only alphanumeric (A-Z, a-z, 0-9), dash (-) or dot (.) characters. Use dots and dashes between alphanumeric characters.
- Consider the fields as required.

These rules apply to the SIP Route Class Naming Authority parameter only:

- Ensure that at least one dot exists.
- After the final dot, ensure the first character is alphabetical (A-Z, a-z) and ensure subsequent characters are alphanumeric or dashes.

Installation/Upgrade (Migration) Considerations

No additional network installation or upgrade considerations exist. Ensure G. Clear codec is enabled on the T1 PRI trunks that require the codec and that the bandwidth override service parameter is enabled for the regions that provide less than 64 kb/s of bandwidth per call.

No new port requirement exists.

Serviceability Considerations

No Cisco Unified Serviceability considerations exist for this feature. This feature requires no new alarms or counts to be added.

AXL and CTI Considerations

AXL supports an optional tag called GClearEnable in the add/update/get MGCP and SIP API; this tag applies to T1 PRI trunks. The user can use the AXL MGCP and SIP API to enable or disable the G. Clear support for T1 PRI trunks.

No CTI considerations exist for this feature.

User Tips

A negligible amount of delay occurs to MGCP processing.

No software, hardware, or firmware restrictions exist.

No accessibility restrictions or special configuration considerations exist.

For More Information

Refer to the following documents for additional configuration details for this feature:

- *Cisco Unified Communications Manager Features and Services Guide, Release 7.0(1)*
- *Cisco Unified Communications Manager Administration Guide, Release 7.0(1)*
- *Cisco Unified Communications Manager System Guide, Release 7.0(1)*

G.729a and G.729b Codecs Over SIP Trunks

You can use G.729a and G.729b, which are low-bandwidth codecs, for calls that are initiated over SIP trunks. Consider this feature as required for endpoints that do not support delayed media calls and do not want to use a higher-bandwidth codec, such as G.711.

Because an MTP needs to be preallocated for early-offer calls, you must configure an external MTP or transcoder device to use this feature. The software MTP does not support G.729 over SIP trunks.

Although this feature supports all four G.729 codecs (G.729, G.729a, G.729b, and G.729ab), the system cannot distinguish between G.729 and G.729a or between G.729b and G.729ab. Therefore, Cisco Unified Communications Manager Administration provides only two options for configuring these codecs on SIP trunks: G729/G729a and G729b/G729ab.

The G.729 codec over SIP trunks applies only to outgoing calls, and incoming calls do not get affected. Be aware that the system does not support mid-call codec switching from G.729 to any other codec.

Cisco Unified Communications Manager Administration Configuration Tips

In Cisco Unified Communications Manager Administration, you can enable G.728a and G.729b codecs for the MTP Preferred Originating Codec.

Note To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. For more information, see "Transcoders" in the *Cisco Unified Communications Manager System Guide*.

This field gets used only when the MTP Termination Point Required check box is checked.

GUI Changes

To access the MTP Preferred Originating Codec parameter, choose **Device > Trunk**.

For More Information

- "Understanding Session Initiation Protocol (SIP)," *Cisco Unified Communications Manager System Guide*
- "Transcoders," *Cisco Unified Communications Manager System Guide*
- "Trunk Configuration," *Cisco Unified Communications Manager Administration Guide*

Enhanced IP Phone Services

The end user can, at the discretion of the Cisco Unified Communications Manager administrator, subscribe to IP Phone Services that are accessible under the Directories and Messages buttons, including the ability to control the presence of standard phone applications such as Call History logs Personal and Corporate Directory.

- IP Phone Services get explicitly provisioned to the phone in its configuration file. Administrators control the provisioning and enabling of services on the phone, including the internal phone applications such as Call History logs.
- An added service type allows services to be provisioned to the Directories and Messages buttons (in addition to existing support for only the Services button).
- The administrator can provision services with Enterprise Subscriptions that apply to all devices and that the user cannot override.
- Added Phone Service parameters allow provisioning of applications that persist in flash on the phone (such as Java MIDlets).
- You can selectively enable and disable services.

Cisco Unified Communications Manager Administration Configuration Tips

To minimize the impact to Cisco Unified Communications Manager performance and call processing, do not put IP phone services on any Cisco Unified Communications Manager server at your site or any server that is associated with Cisco Unified Communications Manager, such as the TFTP server or directory database publisher server. To ensure that variable length calls occur correctly, make sure that you configure the translation patterns as non-urgent.

If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

GUI Changes

The following new fields display in the IP Phone Services Configuration window in Cisco Unified Communications Manager Administration:

- Service Category—Indicates whether the service is based on XML or Java MIDlet.
- Service Type—Determines whether the service is provisioned to the Services, Directories, or Messages button.
- Service Vendor—Used only for Java MIDlet services, must exactly match the vendor that is defined in the MIDlet JAD file.
- Service Version—Optional (if defined for Java MIDlet services, must exactly match the version that is defined in the JAD file).
- Enable check box—Allows the administrator to enable or disable the service without removing it.
- Enterprise Subscription—Automatically provisions the new service to all devices in the enterprise without requiring individual subscription.

The following field displays in the Phone Configuration window:

- Services Provisioning—Determines whether the phone will use the services that are provisioned in the phone configuration file (Internal), services received from an external URL (External URL), or both.

The following field displays in the Common Phone Profile Configuration window:

- Services Provisioning—Determines whether the phone will use the services that are provisioned in the phone configuration file (Internal), services received from an external URL (External URL), or both.

For More Information

- "IP Phone Services Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Common Phone Profile Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Extension Mobility," *Cisco Unified Communications Manager Features and Services Guide*
- "Cisco Unified IP Phone Services," *Cisco Unified Communications Manager System Guide*

Intelligent Bridge Selection

Cisco Unified Communications Manager 7.0 can intelligently select a video conference bridge from the configured Media Resource Group List (MRGL) if two or more of the original conference participants are video enabled. If one or no video participants exists, Cisco Unified Communications Manager selects an audio conference bridge from the configured MRGL.

Cisco Unified Communications Manager selects an audio or a video conference bridge from the configured MRGL of the conference initiator. However, if no MRGL is configured for the conference initiator, Cisco Unified Communications Manager allocates the video or audio conference bridge from the default MRGL.

If a video conference bridge needs to be allocated but none is available, Cisco Unified Communications Manager allocates an audio conference bridge for the conference. Similarly, if an audio conference bridge is needed but is unavailable, Cisco Unified Communications Manager allocates a video conference bridge.

The conference bridge that is allocated depends upon the video capability of the endpoints that are joining the conference.

Note The Intelligent Bridge Selection feature applies only to ad hoc conferences and does not impact how conference bridges are allocated for meet-me conferences. The conference bridge for a meet-me conference gets allocated on the basis of the configured MRGL for the endpoint that initiates the conference. Cisco Unified Communications Manager does not take into account whether the conference initiator is video-capable to allocate a conference bridge for meet-me conference calls.

Cisco Unified Communications Manager Administration Configuration Tips

You need to configure the following service parameters to enable intelligent bridge selection:

- Choose Encrypted Audio Conference Instead of Video Conference—This parameter determines whether Cisco Unified Communications Manager chooses an encrypted audio conference bridge or an unencrypted video conference bridge for an ad hoc conference call when the conference controller Device Security Mode is set to either Authenticated or Encrypted and at least two conference participants are video-capable.
- Minimum Video-Capable Participants to Allocate Video Conference—This parameter specifies the number of video-capable conference participants that must be present in an ad hoc conference for Cisco Unified Communications Manager to allocate a video conference bridge. If the number of video-capable participants is less than the number that this parameter specifies, Cisco Unified Communications Manager allocates an audio conference bridge. If the number of video-capable participants is equal to or greater than the number that this parameter specifies, Cisco Unified Communications Manager allocates a video conference bridge, when available, from the configured media resource group list (MRGL).
- Allocate Video Conference Bridge for Audio-only Conferences when Video Conference Bridge has Higher Priority—This parameter determines whether Cisco Unified Communications Manager chooses a video conference bridge, when available, for an ad hoc audio-only conference call when a video conference bridge has a higher priority than an audio conference bridge in the MRGL.

  If an audio conference bridge has higher priority than any video conference bridge in the MRGL, Cisco Unified Communications Manager ignores this parameter.

  This parameter proves useful in situations where the local conference bridge is a video bridge (and configured in the MRGL with the highest priority) and audio conference bridges are only available in remote locations. In such a situation, enabling this parameter enables Cisco Unified Communications Manager to attempt to use the local video conference bridge first, even for audio-only conference calls.

For More Information

For information on Intelligent Bridge Selection features in Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager System Guide*, *Release 7.0(1)*.

International Escape Character + Support

Configuring the international escape character, +, in Cisco Unified Communications Manager Administration allows your phone users to place calls without having to remember and enter the international direct dialing prefix/international escape code that is associated with the called party. Depending on the phone model, for example, dual-mode phones, your phone users can dial + on the keypad of the phone. In other cases, the phone user can return calls by accessing the call log directory entries that contain +. In addition, using the international escape character allows you to support globalization of calling party numbers, which is part of the calling party normalization feature. For information on the calling party normalization feature, see the "Calling Party Normalization" section on page 44.

The international escape character, +, signifies the international access code in a complete E.164 number format. For example, NANP numbers have an E.164 global format in the format +1 214 555 1234. The + acts as a leading character that service providers replace in different countries with the international access code to achieve global dial plans.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

To configure the international escape character, +, for patterns and directory numbers, you configure \+ in the windows in Table 4:

Table 4 Entering \+ in Cisco Unified Communications Manager Administration

Configuration Window	Fields That Support Entering \+ for International Escape Character
Route Pattern, Hunt Pilot, and Translation Pattern	Route Pattern, Hunt Pilot, and Translation Pattern
Directory Number	Directory Number
Intercom Translation Pattern	Intercom Translation Pattern
Calling Party Transformation	Pattern
Called Party Transformation	Pattern

Entering + in the windows in Table 4 does not configure the international escape character; instead, entering the + in the pattern fields means that the system should match one or more of the earlier characters during digit analysis, as described in the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco Unified Communications Manager System Guide*. Consider the following information for configuring the international escape character in the windows in Table 4:

- To configure the international escape character for supported patterns, make sure that you enter \+ in the pattern or Directory Number field.
- For all patterns in Table 4 except for the directory number, you can configure the international escape character, \+, at the beginning, in the middle, or at the end of a pattern. For example, you can configure \+91! or 0\+23! in the pattern fields.

  For directory numbers, you can configure the international escape character, \+, at the beginning of the number only.
- You can configure \+ as a dialable character and a + wildcard within a single pattern; for example, you can configure a pattern like 1234\+56+, where \+ equals the dialable character and + serves as the wildcard.
- You can configure multiple international escape characters \+ in a single pattern; for example, you can configure a pattern like 147\+56\+89\+.

Tip Meet-Me patterns, Call Park (and related call park features; for example, Directed Call Park) patterns, and Call Pickup patterns do not support the international escape character, +, so you cannot enter \+ in the pattern fields that are configured for these features.

Table 5 provides the configuration windows and fields where you can enter + to indicate the international escape character +.

Table 5 Configuring + for the International Escape Character in Cisco Unified Communications Manager Administration

Configuration Window	Fields That Support Entering + for International Escape Character
Device Pool	Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix
Service Parameter	All Incoming Prefix fields
Route Pattern, Hunt Pilot, Intercom Translation Pattern, and Translation Pattern	Calling Party Transform Mask, Called Party Transform Mask, and Prefix Digits (Outgoing Calls)
Access List Member Detail	DN Mask field
Directory Number	External Phone Number Mask and all Call Forwarding fields
Calling Party Transformation	Calling Party Transform Mask and Prefix Digits (Outgoing Calls)
Called Party Transformation	Called Party Transform Mask and Prefix Digits
Voice Mail Port and Voice Mail Port Wizard	External Number Mask
Message Waiting	Message Waiting Number
Voice Mail Pilot	Voice Mail Pilot Number
Gateway	Prefix fields, which include Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix; Caller ID DN, and Prefix DN **Tip** MGCP gateways support sending the international escape character + ; H.323 gateways do not support the +, so the gateway strips the + when a calling or called party offers it to the gateway.
Trunk	Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and Incoming Calling Party Subscriber Number Prefix; SIP trunk only supports the Incoming Calling Party Unknown Number Prefix. Caller ID DN and Prefix DN
Speed Dial and Abbreviated Dial	Number (allows the international escape character, +, to display as part of the speed dial number on the phone)

SIP and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +, but SIP trunks can support sending the +.

For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the gateway strips the + when Cisco Unified Communications Manager sends the call information to the gateway.

When + is not supported but the global calling party number includes +, configure the called party transformations and route patterns to send the outdial digits in a format that the device supports.

Service Parameter and Enterprise Parameter Changes

If you want to do so, you can configure the Strip + on Outbound Calls service parameter, which supports the Cisco CallManager service. This parameter determines whether Cisco Unified Communications Manager strips the international escape character, +, from the calling and called parties for outgoing calls through MGCP gateways and SIP trunks. If your network or far-end gateway does not recognize the + as a digit, set this parameter to False; if you set this parameter to True and the + is not supported in network or by the receiving gateway, calls that use + may drop. Ensure that calls over QSIG trunks do not utilize + because QSIG does not send the +. This parameter does not impact H.323 outbound calls because H.323 gateways unconditionally strip the + when they route outbound calls.

If you set the Strip + on Outbound Calls service parameter to True, Cisco Unified Communications Manager strips the + for the calling and called parties for all outgoing calls through all MGCP gateways and SIP trunks. To ensure that Cisco Unified Communications Manager does not strip the + for outgoing calls through particular MGCP gateways and SIP trunks, configure the calling party and called party transformation patterns for outgoing gateways to include the + prefix for international calls.

Installation/Upgrade (Migration) Considerations

After you upgrade to Cisco Unified Communications Manager 7.0, you may need to update your dial plans, speed dials, and so on, in Cisco Unified Communications Manager Administration to support the international escape character +.

Serviceability Considerations

Make sure that the Cisco CallManager service is activated in Cisco Unified Serviceability.

BAT Considerations

You can configure the incoming prefix fields for phones in the Bulk Administration Tool.

CAR/CDR Considerations

For information on how the international escape character + works with CDRs and Cisco Unified Communications Manager CDR Analysis and Reporting, see the "Cisco Unified Communications Manager CDR Analysis and Reporting" section on page 112 and the "Cisco Unified Communications Manager Call Detail Records" section on page 118.

User Tips

The following Cisco Unified IP Phones, which run SIP or SCCP unless noted otherwise, can display + on the phone screen, speed dials, directory numbers, and in call log (Redial, Missed Calls, and so on) directories on the phone.

- 7906 and 7911
- 7921G (SCCP only) and 7931
- 7941, 7942, 7945

- 7961, 7965
- 7970, 7971, 7975
- 7985 (SCCP only)

The Nokia S60, a dual-mode phone, also supports + dialing from the keypad on the phone. For example, a caller in the United States calls an international number in India. If the caller uses a dual-mode phone, the caller can directly dial + to represent the international number. The caller may call 0+91802501523 or +91802501523, depending on the outgoing route pattern settings. Dialing the + on the keypad assumes that the outgoing gateway can support the +; if the outgoing gateway does not support +, you must configure the route pattern like \+!, where Cisco Unified Communications Manager strips the \+ and prefixes 011 to transform the international number to 011 91 802501523.

Consider the following information about + and the phone:

- If a phone displays the + in a call log directory entry on the phone, the end user can place a call without having to edit the entry in the call log directory. If the outgoing gateway does not support the +, configure the outgoing route pattern, so Cisco Unified Communications Manager can strip the international escape code and prefix the international access code to the directory number in the call log directory.
- If you do not configure transformation patterns to localize the calling party number, as described in "Localizing the Calling Party Number" section in the *Cisco Unified Communications Manager Features and Services Guide*, a called party may receive an international call that contains + in the calling party number, for example, 0+494692022002 or +4940692022002, depending on the configuration of the incoming gateway. If the called party does not answer the call, the calling party number gets stored with the + in the call log directories on the phone. The called party can return the call without having to edit the entry in the call log directory.
- A caller can place a call to a speed dial number that is configured as an E.164 number that contains the +.
- Cisco Unified IP Phones 7902, 7905, 7912, 7920, 7940, and 7960 that run SCCP can receive calls from directory numbers that contain the international escape character, +, although these phones do not display the + on the phone because Cisco Unified Communications Manager strips the + before the call completes.
- SRST does not work for phones that are running SIP that display the + in the call alerting pane or the call log directories on the phone; therefore, phones that are running SIP that display the + cannot register with SRST-enabled gateways, and calls to the SRST-enabled gateway fail if a directory number that is used for the call includes the +. Phones that are running SCCP that display the + on the phone can register with SRST.
- In the Cisco Unified CM User Options, an end user can configure + for fast dials and speed dials.

For More Information

- "Understanding Route Plans," *Cisco Unified Communications Manager System Guide*
- "Calling Party Normalization," *Cisco Unified Communications Manager Features and Services Guide*
- Calling Party Normalization, page 44
- Non-Urgent Translation Patterns, page 88
- Cisco Unified Mobility Chapter Omits Information about the DN Mask Field, page 173

LDAP Support in Cisco Unified Communications Manager Business Edition

The Cisco Unity Connection directory comes from Cisco Unified Communications Manager; that is, components in Cisco Unity Connection synchronize directory updates from Cisco Unified Communications Manager to Cisco Unity Connection.

If you enable LDAP synchronization and activate the DirSync service in Cisco Unified Serviceability, the DirSync service in Cisco Unified Communications Manager synchronizes corporate directory data for Cisco Unified Communications Manager and Cisco Unity Connection to the Cisco Unified Communications Manager database. With LDAP synchronization, Cisco Unity Connection does not know that the user information came from LDAP; instead, Cisco Unity Connection views users as Cisco Unified Communications Manager users.

Cisco Unified Communications Manager allows synchronization from Microsoft Active Directory 2000 and Microsoft Active Directory 2003, Microsoft Active Directory 2008, iPlanet Directory Server 5.1, Sun ONE Directory Server 5.2, and Sun Java System Directory Server 6.0, 6.1, and 6.2 to the Cisco Unified Communications Manager database.

LDAP synchronization applies only to end users; LDAP synchronization does not affect application users.

A DirSync that is invoked for Microsoft Active Directory performs a complete (total) synchronization of data.

Cisco Unified Communications Manager allows the following options:

- Automatic synchronization, which synchronizes the data at regular intervals.
- Manual synchronization, which allows forcing the synchronization.
- Stop synchronization, which stops the current synchronization. If synchronization is in progress, check for agreement.

LDAP authentication in Cisco Unified Communications Manager verifies the identity of the user by validating the user ID and password/PIN before granting access to the system. Verification takes place against the Cisco Unified Communications Manager database or the LDAP corporate directory.

GUI Changes

LDAP support occurs in the following windows in Cisco Unified Communications Manager Administration:

- LDAP System Configuration—Access this window to enable or disable synchronization from the LDAP server and to configure the LDAP server type and the LDAP attribute for user ID. Choose **System > LDAP > LDAP System** to display the LDAP System Configuration window.
- LDAP Directory—Access this window to configure attributes for the LDAP directory. Choose **System > LDAP > LDAP Directory** to display the Find and List LDAP Directories window.
- LDAP Authentication Configuration—Use the LDAP Authentication Configuration window to configure LDAP authentication settings. Use this window to enable or disable LDAP authentication for end users as well as to provide LDAP server information. Choose **System > LDAP > LDAP Authentication** to display the LDAP Authentication window.

Cisco Unified Communications Manager Administration Configuration Tips

After the LDAP user gets synchronized in Cisco Unified Communications Manager, you must manually create the user in Cisco Unity Connection Administration. To manually create the user, perform one of the following tasks:

- Import the user into Cisco Unity Connection by configuring Cisco Unity Connection Administration, as described in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection.*
- Choose **User Management > End User** in Cisco Unified Communications Manager Administration and create the Cisco Unity Connection mailbox, as described in the "Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox" section in the *Cisco Unified Communications Manager Administration Guide*.

When you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you cannot change web passwords from Cisco Unity Connection Administration.

You cannot delete an end user in Cisco Unity Connection Administration, unless you have enabled LDAP synchronization and the Cisco DirSync service deletes the user in Cisco Unified Communications Manager Administration after you delete the user in the LDAP directory. If the Cisco DirSync service deletes the user for Cisco Unified Communications Manager, you must manually delete the user in Cisco Unity Connection, as described in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection.* If you do not delete the user in Cisco Unity Connection Administration, Cisco Unity Connection classifies the user as orphaned.

You can make changes to LDAP Directory information and LDAP Authentication settings only if synchronization from the customer LDAP directory is enabled in the LDAP System window in Cisco Unified Communications Manager Administration. Conversely, if you want to enable administrators to modify LDAP directory information and LDAP authorization settings, you must disable synchronization with the LDAP server in Cisco Unified Communications Manager Administration.

After an LDAP Directory configuration for the DirSync service gets created or the LDAP user authentication is enabled, the settings in the LDAP System window display as read only.

When you configure a user in the corporate directory, ensure that you configure a last name for the user. After you configure LDAP synchronization in Cisco Unified Communications Manager Administration, users without last names in the corporate directory do not synchronize with the Cisco Unified Communications Manager database. No error displays in Cisco Unified Communications Manager Administration, but the log file indicates which users did not synchronize.

Although you enable synchronization in the LDAP Synchronization window, you configure the synchronization method (automatic, manual, or stopped) in the LDAP Directory window.

After you configure the LDAP directory or enable LDAP user authentication in Cisco Unified Communications Manager Administration, the settings in the LDAP System Configuration window display as read only.

Checking the Enable Synchronizing from LDAP Server check box in LDAP System Configuration window prevents you from updating end user information in the End User Configuration window in Cisco Unified Communications Manager Administration. You can update end user data only in the corporate directory itself, after which you should perform a resynchronization.

When you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you cannot change web passwords from Cisco Unity Connection Administration.

If end users exist in the Cisco Unified Communications Manager database before synchronization with a corporate directory occurs, the system deletes those end users that did not have a matching user ID in the corporate directory. For example, if users *bob* and *sanjay* were in the Cisco Unified Communications Manager database, but only *bob* was in the LDAP directory, then *sanjay* gets marked inactive and eventually get deleted by the garbage collector program.

To use only the Cisco Unified Communications Manager database for users, which is the default functionality when you install Cisco Unified Communications Manager, create users with End User Configuration to add to the database (password, names, device association, and so forth). Authentication

takes place against the information that is configured in Cisco Unified Communications Manager Administration. End users and administrators can make password changes if this method is used. This method does not entail LDAP synchronization.

For users to use their LDAP corporate directory passwords, you must configure LDAP authentication (**System > LDAP > LDAP Authentication**).

Service Parameter and Enterprise Parameter Changes

You can configure service parameters for the Cisco DirSync service. To access the service parameters, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. In the window that displays, choose a server in the Server drop-down list box. In the Service drop-down list box, choose the **Cisco DirSync** service. The Service Parameter Configuration window allows configuration of the Cisco DirSync service parameters. For information on the service parameters, click the question-mark button that displays in the upper, right corner of the window.

Installation/Upgrade (Migration) Considerations

By default, Cisco Unified Communications Manager uses any end user information in the End User Configuration window in Cisco Unified Communications Manager Administration until you synchronize the corporate directory with the Cisco Unified Communications Manager database.

Serviceability Considerations

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service in Cisco Unified Serviceability. If you enable LDAP synchronization and you need to enable trace for the directory, you must enable trace for the DirSync service in Cisco Unified Serviceability and enable trace for the CuCmDbEventListener component in Cisco Unity Connection Serviceability.

In Cisco Unified Serviceability, you can enable trace for the Cisco Dirsync service by choosing **Trace > Configuration**. In the Trace Configuration window, choose the server where the Cisco Dirsync service is activated and click **Go**. Then, choose **Directory Services** from the Service Group drop-down list box and click **Go**. Then, choose the Cisco DirSync service and click **Go**. For more information on configuring trace, refer to the *Cisco Unified Serviceability Administration Guide*,

To view traces, you use the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool. For information on viewing traces, refer to the *Real-Time Monitoring Tool Administration Guide*.

BAT Considerations

If you use your corporate directory and have Lightweight Directory Access Protocol (LDAP) synchronization enabled in Cisco Unified Communications Manager Administration, you cannot use BAT to insert/update or delete users.

User Tips

When both synchronization and LDAP authentication are enabled, the system always authenticates application users and end user PINs against the Cisco Unified Communications Manager database. End user passwords get authenticated against the corporate directory; thus, end users need to use their corporate directory password.

When only synchronization is enabled (and LDAP authentication is not enabled), end users get authenticated against the Cisco Unified Communications Manager database. In this case, you configure a password by using the Cisco Unified Communications Manager Administration End User Configuration window.

Keep in mind that configuring authentication is optional. If authentication is not enabled, administrators and end users have two passwords, an Active Directory or Netscape Directory password and a Cisco Unified Communications Manager password.

For More Information

- "Understanding the Directory," *Cisco Unified Communications Manager System Guide for Cisco Unified Communications Manager Business Edition*
- "LDAP System Configuration," *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*
- "LDAP Directory Configuration," *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*
- "LDAP Authentication Configuration," *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*

Local Route Groups

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

Release 7.0 of Cisco Unified Communications Manager introduces a special Local Route Group that can be bound to a provisioned route group differently based on the Local Route Group device pool setting of the originating device. Devices, such as phones, from different locales can therefore use identical route lists and route patterns, but Cisco Unified Communications Manager selects the correct gateway(s) for their local end.

Note This document uses the term *provisioned route group* to specify a route group that an administrator configures through use of the **Call Routing > Route/Hunt > Route Group** menu option in Cisco Unified Communications Manager Administration.

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).

In simple local routing cases, the provisioning gets reduced from N route patterns and N route lists to one route pattern and one route list. In cases with Tail End Hop Off (TEHO), local route groups allow configuration of N route patterns and N route lists instead of N^2 route patterns and N^2 route lists. Because values for N can reach much more than 1000 for larger implementations, enormous scalability savings result.

In earlier releases, Cisco Unified Communications Manager treated gateways as devices to which multiple patterns are assigned. A tight, somewhat inflexible, binding existed between a gateway and the patterns that Cisco Unified Communications Manager associated with the gateway. When a call was placed, Cisco Unified Communications Manager viewed the situation as "Caller X has dialed some digits. These digits match pattern Y. Pattern Y directly associates with route lists, route groups, and gateways A, B, and C."

When the administrator adds a new route group to a route list, the Route List Configuration window presents the administrator with all available route groups from which to select. This list includes as its first member the special route group that is named *Standard Local Route Group*. This local route group specifies a virtual local route group.

The local route group does not statically get bound to any provisioned route group. The local route group does not display in the Find and List Route Groups configuration window, and, therefore, cannot be deleted or modified. You can, however, add the local route group to any route list; when so added, the local route group serves as a placeholder for a provisioned route group that will later get bound to the local route group dynamically during call setup.

Binding Provisioned Route Group to a Local Route Group During a Call

Deferring the binding of a provisioned route group to the local route group until call setup ensures that the desired provisioned route group can be the one that is local to the device that is placing the call. Thus, a device in location X would use a provisioned route group that contains gateways for the location X PSTN while a device in location Y would use a different provisioned group of gateways for the location Y PSTN.

You need to ensure that each device in the system is provisioned to know its local route group. To avoid specifying this information in the configuration window for each device, because the number of devices can be many thousands, Cisco Unified Communications Manager Administration locates the information in the device pool for the device, because device pools specify common site-specific information.

The Local Route Group field in the Device Pool Configuration window includes a drop-down list box that lists all available (provisioned) route groups. This list excludes the special Standard Local Route Group name (because only provisioned route groups should be configured for a device pool) but presents the special name, <NONE>, which specifies the first (default) choice. Choose <NONE> if no binding is desired.

Whenever the default value <NONE> is selected for a device pool, any call that uses a route list that includes the local route group, Standard Local Route Group, gets routed as if the Standard Local Route Group is absent from the list.

With this mechanism, a call that is placed from any device over a route list that contains the special Standard Local Route Group behaves as follows:

1. The route list algorithm searches through the list of included route groups, in the designated order, until an unused trunk can be found. (The earlier and current implementations do not differ.)
2. If the search encounters the special Standard Local Route Group, the system automatically replaces this route group with the name of the local route group that is provisioned for the calling device, unless the search encounters one of the following situations:
   - If the provisioned route group specifies <NONE>, the Standard Local Route Group gets skipped entirely.
   - If by skipping the Standard Local Route Group in this way, the search ends (that is, the Standard Local Route Group comprises the last or only route group in the route list), routing aborts, and the user receives reorder tone or an equivalent notification.

Routing With Local Route Groups

With local route group mapping, Cisco Unified Communications Manager can treat gateways more like a service.

Simple Local Routing

Simple local routing comprises cases in which each site needs to route offnet calls to its local gateways. Provisioning of route patterns and route lists can get reduced from the need to configure N route patterns and N route lists to a configuration in which only one route pattern and one route list are needed.

For this case, assume that all phones that home to a particular site belong to a single calling search space (CSS) that is unique to that site. For example, phones at the Boulder site belong to the CSS-Bldr calling search space and so forth. Without using the Local Route Group feature, regardless of site, a phone always prefers its local gateway when making an offnet call by dialing 9 followed by a 7-, 10-, or 11-digit pattern. As more sites get added, each column must include new entries (rows). If N sites exist, you need N different route lists, route patterns, partitions, and calling search spaces.

In the same implementation, use of the Local Route Group feature allows configuration of a single route list, partition, route pattern, and CSS, regardless of the number of sites. In this case, the following configuration applies:

- All phones belong to a single CSS-System calling search space and to a single P-System partition.
- All phones for a given site belong to a single device pool unique to that site.
- The Local Route Group field in each device pool identifies the specific route group for that site. In this example, RG-Bldr for Boulder, RG-Rch for Richardson, and so on.

Thus, the route lists, route patterns, partitions and calling search spaces for this case each get reduced from N to 1. The number of gateways, route groups, and device pools remain N for N sites.

A new partition, P_System, and a new calling search space, CSS_System, get added for accessing the 9.@ pattern from all sites. The calling search space, CSS_Boulder, can contain both P_Boulder and P_System as well, as can the CSS of the other sites.

Tail End Hop Off

Tail End Hop Off (TEHO) refers to routing long-distance calls across the VoIP network and dropping them off to the Public Switched Telephone Network (PSTN), as a local call, at a remote gateway. In TEHO situations, the configuration complexity can get reduced from the need to configure N^2 entities to needing only N entities. The following assumptions for TEHO apply:

- Each site has a different route pattern and route list for each of the other N-1 sites.
- For a given site, S, each of the N-1 route lists to another (remote) site has, as first preference, a route group of one or more gateways that are local to that other site followed by, as second preference, a route group that is local to S. Therefore, when sufficient trunking resources are available to honor the first preference, a long-distance call uses a gateway at the remote site to go offnet and thus bypass any tolls; otherwise, the call defaults to a local gateway and incurs toll charges.

Again, Cisco Unified Communications Manager uses an identical routing policy for all sites. The second preference of routing a call through the local PSTN of a site (if the system fails to drop off the call as a local call at the remote PSTN) forces the customer to provision separate instances of all routing information for each site. Each site includes a unique set of route patterns and route lists to each of the other N-1 sites, as well as a generic local route list for all other calls that the remote access codes do not cover. This requirement entails a total of $N \times (N-1)+N$, or N^2, route lists and route patterns for the general case.

Using the Local Route Group feature, the $N \times (N-1)$ route patterns and route lists that are needed for remote sites reduce to N, and the N local route patterns and local route lists reduce to 1. Overall, the total number of route lists and route patterns decreases from N^2 to N+1, and calling search spaces and partitions decrease from N to 1.

The crucial mechanism specifies the use of the *Standard Local Route Group* as the second choice in each route list. The setting in the device pool of the originating device dynamically determines the actual provisioned route group that gets used during a specific call.

Called Party Transformations

While loose coupling occurs between the enterprise number and the route group/gateway, very tight coupling occurs between the route group/gateway and the patterns that the PSTN expects. If the gateway chosen is in a 7-digit dialing location, the PSTN expects 7 digits; if the chosen gateway is in a 10-digit location, the PSTN expects 10 digits to access local numbers.

Called Party Transformation Example 1

A call gets placed from Dallas; the called number specifies 9.5551212. If the Dallas local gateway is busy or not accessible, assuming that the San Jose gateway is selected, 9.5551212 must be converted to 1 214 555 1212 for the San Jose gateway to dial out.

In the same example for a Local Route Group case, a call is placed from Dallas. The called number is 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed by the originator, discard PreDot, and insert the prefix +1 214.
2. Convert the call number to a globally unique E.164 string (+1 214 555 1212).

If a San Jose gateway gets selected, the system converts the global string +1 214 555 1212 to 1 214 555 1212; if a Dallas gateway gets selected, the system converts the global string to 214 555 1212.

Called Party Transformation Example 2

A call gets placed from RTP; the called number specifies 5551212. If the RTP local gateway is busy or not accessible, and if it is assumed that the San Jose gateway is selected, 5551212 must get converted to 1 919 555 1212 for the San Jose gateway to dial out.

In the same example for a Local Route Group case, a call gets placed from RTP. The called number specifies 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed, discard PreDot, and insert the Prefix 91919.
2. Convert the called number to a global dialing string (9 1 919 555 1212).

If a San Jose gateway gets selected, the system converts the global string 91 919 555 1212 to 1 919 555 1212; if the RTP gateway gets selected, the system converts the global string to 555 1212.

Cisco Unified Communications Manager Administration Configuration Tips

When the administrator adds a new route group to a route list, the Route List Configuration window presents the administrator all available route groups from which to select. This list includes as its first member the special route group that is named *Standard Local Route Group*. This local route group specifies a virtual local route group.

Be aware that the local route group is not statically bound to any provisioned route group. The local route group does not display in the Find and List Route Groups configuration window and therefore cannot be deleted or modified. The local route group can, however, get added to any route list; when so added, the local route group serves as a placeholder for a provisioned route group that will later be bound to the local route group dynamically during call setup.

After it is added to a route list, the local route group can get removed later from that list, or its search-order place in the list can get modified as with any provisioned route group.

GUI Changes

The local route groups feature involves the following new and changed settings in the Cisco Unified Communications Manager Administration GUI:

- **System > Device Pool**—The Device Pool Configuration window adds the Local Route Group, Calling Party Transformation CSS, and Called Party Transformation CSS settings.
- **Call Routing > Route/Hunt > Route List**—The Route List Configuration window adds the Standard Local Route Group choice in the Selected Route Groups pane of the Route List Member Information area.
- **Call Routing > Transformation Pattern > Calling Party Transformation Pattern**—This new menu option replaces the **Call Routing > Transformation Pattern Configuration** option.
- **Call Routing > Transformation Pattern > Called Party Transformation Pattern**—This represents a new menu option.
- **Device > Gateway**—The Gateway Configuration window adds the Called Party Transformation CSS setting.
- **Device > Trunk**—The Trunk Configuration window adds the Called Party Transformation CSS setting.

Service Parameter and Enterprise Parameter Changes

No service parameter changes nor enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation considerations exist for this feature.

When you upgrade from an earlier release of Cisco Unified Communications Manager, the new Standard Local Route Group field gets initialized to the default setting, NULL, for <NONE>.

Serviceability Considerations

This feature affects the Cisco Dialed Number Analyzer service within Cisco Unified Serviceability.

CAR/CDR Considerations

This feature causes the final transformed called party number to be reported in the CDR records.

AXL and CTI Considerations

This feature entails the following AXL requirements:

- AXL supports the new optional parameter, Local Route Group (DevicePool.fkRouteGroup_Local), in add/update/get DevicePool API. The new tag specifies localRouteGroup. This new tag accepts Pkid attribute or name in add/update requests.
- AXL supports the new optional parameter, Called Party Transformation CSS (DevicePool.fkCallingSearchSpace_CdPNTranformation), in add/update/get DevicePool API. The new tag specifies cdpnTransformationCSS. This new tag accepts Pkid attribute or name in add/update requests.
- AXL supports the new optional parameter, Called Party Transformation CSS (Device.fkCallingSearchSpace_CdPNTranformation), in add/update/get MGCPEndPoint/SIPTrunk/H323Trunk/H323Gateway API. The new tag specifies cdpnTransformationCSS. This new tag accepts Pkid attribute or name in add/update requests.

- AXL supports the new optional Boolean parameter, Use Device Pool CdPN Transformation CSS (Device.useDevicePoolCdpnTransformCSS), in add/update/get MGCPEndPoint/SIPTrunk/H323Trunk/H323Gateway API. The new tag specifies useDevicePoolCdpnTransformCSS.
- AXL supports add/update/get/remove Called Party Transformation. This new API contains the following fields: Pattern, Partition, Description, Numbering Plan, Route Filter, Urgent Priority (Read Only) Discard Digits, Called Party Transformation Mask, Prefix Digits, Called Party IE Number Type, and Called Party Numbering Plan. This new API specifies add/update/get/remove CalledPartyTransformation.

No CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

For More Information

- "Local Route Groups," *Cisco Unified Communications Manager Features and Services Guide*
- "System-Level Configuration Settings," *Cisco Unified Communications Manager System Guide*
- "Partitions and Calling Search Spaces," *Cisco Unified Communications Manager System Guide*
- "Understanding Route Plans," *Cisco Unified Communications Manager System Guide*
- "Understanding Cisco Unified Communications Manager Voice Gateways," *Cisco Unified Communications Manager System Guide*
- "Device Pool Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route Group Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route List Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Route Plan Report," *Cisco Unified Communications Manager Administration Guide*
- "Calling Party Transformation Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Called Party Transformation Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Gateway Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Trunk Configuration," *Cisco Unified Communications Manager Administration Guide*

Non-Urgent Translation Patterns

In earlier releases Cisco Unified Communications Manager prioritized translation patterns as urgent; that is, Cisco Unified Communications Manager routed the call as soon as digit analysis identified a match with the translation pattern. Because Cisco Unified Communications Manager 7.0 supports local route groups, calling party normalization, and the international escape character +, which allow you to globalize, route, and localize calling party numbers, you can configure translation patterns as urgent or non-urgent to ensure that Cisco Unified Communications Manager does not route the call before it should be routed.

For example, if a caller in the 408 area code dials 95551212, this number gets globalized to +14085551212 through the use of translation patterns; that is, digit analysis does a pattern match for that string to determine where to route the call. In this example, a translation pattern takes 9.[2-9]XXXXXX,

translates that string to +1408XXXXXXX, and then maps that value to a calling search space that contains the globalized patterns. This example works as long as you do not use variable-length dialing, as is the case with international calls. If you want to route an international call, you need a translation pattern for 9011.! that disregards the predot and adds the prefix +. If you configure the translation pattern as urgent priority, 9011! matches with the first digit after the 9011, and Cisco Unified Communications Manager attempts to route the call without waiting to match more digits. As a result, international and any other variable length calls do not route correctly.

Cisco Unified Communications Manager Administration Configuration Tips

In earlier releases of Cisco Unified Communications Manager, Cisco Unified Communications Manager did not allow you to configure similar translation patterns, for example, 9.XXXX and 9.XXXXX, in the same partition because the urgent priority configuration for the translation pattern ensured that digit analysis never matched the second pattern, in this case, 9.XXXXX. Because you can configure translation patterns as non-urgent in Cisco Unified Communications Manager 7.0, you can configure similar translation patterns in the same partition and ensure that digit analysis can accurately match the patterns. Even if digit analysis identifies a match with a translation pattern, Cisco Unified Communications Manager attempts to match more digits in other translation patterns if you configure the translation pattern as non-urgent.

To route international and variable-length calls correctly, make sure that you configure the translation patterns as non-urgent.

GUI Changes

In Cisco Unified Communications Manager Administration, you can configure any translation pattern as urgent priority or non-urgent priority. The Urgent Priority check box displays in the Translation Pattern Configuration (Call Routing > Translation Pattern) and Intercom Translation Pattern Configuration windows (Call Routing > Intercom > Intercom Translation Pattern). If you do not check this check box and if the dial plan contains overlapping translation patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). To interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately, check this check box.

Installation/Upgrade (Migration) Considerations

After you install or upgrade Cisco Unified Communications Manager, the Urgent Priority check box in translation patterns displays as checked and enabled. Update your translation patterns, if necessary, to accommodate your dial plan.

Serviceability Considerations

For call routing to work, you must activate the Cisco CallManager service in Cisco Unified Serviceability.

For More Information

- Calling Party Normalization, page 44
- International Escape Character + Support, page 76
- "Intercom Translation Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Translation Pattern Configuration," *Cisco Unified Communications Manager Administration Guide*

Privacy Headers for SIP Trunks

You can configure four new SIP trunk options to determine what type of privacy information will get included in SIP messages.

GUI Changes

To configure the four options in Cisco Unified Communications Manager Administration, choose **Device > Trunk > SIP Trunk** configuration. Find the four options in the Call Routing pane of the SIP Trunk configuration window:

- Remote-Party-Id—Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Cisco Unified Communications Manager to the remote destination. If you check this box, the SIP trunk always sends the RPID header. If you do not check this box, the SIP trunk does not send the RPID header.
- Asserted-Identity—Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you check this check box, the SIP trunk always sends the Asserted-Type header; whether the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. If the check box is not selected, the SIP trunk does not include any Asserted-Type or SIP Privacy headers in its SIP messages.
- Asserted-Type—Use this drop-down list to choose one of the following values to indicate the type of Asserted Identity header that SIP trunk messages should contain:
  - Default—The default screening indication that comes from Cisco Unified Communications Manager call control
  - PAI (Privacy-Asserted Identity header)
  - PPI (Privacy Preferred Identity header)
- SIP Privacy—Use this drop-down list to choose one of the following values to indicate the type of SIP Privacy header that SIP trunk messages should contain:
  - Default—The Name/Number presentation that comes from Cisco Unified Communications Manager call control
  - None—The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Cisco Unified Communications Manager.
  - ID—The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Cisco Unified Communications Manager.
  - ID Critical—The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label **critical** implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Cisco Unified Communications Manager.

For More Information

Refer to the *Cisco Unified Communications Manager Administration Guide, "Trunk Configuration chapter, "Trunk Configuration Settings for SIP Trunks"* table.

SIP Support for Cisco Unified Communications Manager Features

Cisco Unified Communications Manager 7.0 adds SIP support for features that were previously only available on phones that were running SCCP.

The following features now get supported on phones that are running SIP:

- Single Button Barge/cBarge
- Join and Join Across Lines
- Programmable Line Keys
- Malicious Call ID (MCID)
- Single Call User Interface
- Directed Call Pickup
- Unified Mobile Communications Server (UMCS) Integration
- Do Not Disturb (DND) Call Reject
- Busy Lamp Field (BLF) Alerting and Pickup
- Calling Party Normalization
- International Escape Character + Support

Cisco Unified Communications Manager Administration Configuration Tips

Configuration of the SIP features match the configuration for the equivalent SCCP features.

User Tips

Notify your end users that they can use these features.

For More Information

- "Understanding Session Initiation Protocol (SIP)," *Cisco Unified Communications Manager System Guide*
- Calling Party Normalization, page 44
- Directed Call Pickup, page 65
- International Escape Character + Support, page 76
- Do Not Disturb Call Reject, page 67

SIP T.38 Interoperability with Microsoft Exchange

The T.38 standard comes from the ITU-T Recommendation for real-time transfer of Group 3 facsimile (fax) communication over IP networks. In Cisco Unified Communications Manager, the implementation of T.38 interoperability with Microsoft Exchange enables the system to switch a call from audio to T.38 fax.

The following steps show how the Microsoft Exchange Server establishes a call to a fax machine:

a. The exchange server establishes an audio call with the fax machine.

b. The fax machine send fax tones (CNG) to the exchange server.

c. The exchange server recognizes the fax tones and tries to renegotiate the call as a T.38 fax call.

Cisco Unified Communications Manager Administration allows you to configure a SIP Profile that supports T.38 fax communication. This profile applies to SIP trunks only, not phones that are running SIP or endpoints.

Cisco Unified Communications Manager Administration Configuration Tips

The **Outgoing T.38 INVITE Include Audio mline** parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, you must also configure a SIP trunk with this SIP profile.

GUI Changes

To access the **Outgoing T.38 INVITE Include Audio mline** parameter, choose **Device > Device Settings > SIP Profile**.

For More Information

- "SIP Profile Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Understanding Session Initiation Protocol (SIP)," *Cisco Unified Communications Manager System Guide*

Trusted Relay Points

You can deploy the Cisco Unified Communications system in a network virtualization environment. Cisco Unified Communications Manager enables the insertion of trusted relay points (TRPs). The insertion of TRPs into the media path constitutes a first step toward VoIP deployment within a virtual network.

The underlying network infrastructure comprises one of the key shared assets in an overall network design. A number of customer use cases require support for network infrastructure virtualization, such as the following examples:

- Guest internet access
- Partner access
- Departmental or divisional separation
- Subsidiaries/mergers and acquisitions
- Application segregation (data/voice)

All these applications include a requirement to maintain traffic separation on the network device as well as between network devices.

Traffic separation translates into concepts such as Virtual Routing and Forwarding (VRF). VRF allows multiple instances of a routing table to co-exist within the same router at the same time. In a virtualized network, these different routing domains, or VRFs, typically cannot communicate directly without going through the data center. This situation challenges applications such as Cisco Unified Communications, where devices in the data VRF domain, such as software endpoints that are running on PCs, need to communicate directly with hard phones in the voice VRF domain without hairpinning media in the data center and without directly exposing the voice and data VRFs to each other.

Quality-of-Service Enforcement

In a Cisco voice network, the switch detects Cisco Unified IP Phones that use Cisco Discovery Protocol (CDP), and the switch trusts the Differentiated Services Code Point (DSCP) marking of packets that the Cisco Unified IP Phones send. Because CDP is not secure and can easily be replicated from a PC, the

switch generally does not trust the traffic that is coming from a PC. Because it is almost impossible to ensure that only Cisco Unified Communications Manager-authorized traffic will get marked with DSCP, the packets that come from a PC get re-marked to best effort.

To resolve this problem, Cisco Unified Communications Manager inserts a trusted relay point (TRP) in front of the softphone that runs on the PC, and the media stream from the endpoint can be forced to flow through the TRP. The TRP re-marks the DSCP according to instructions from Cisco Unified Communications Manager. The switch honors and trusts media packets that are sent from the TRP.

Cisco Unified Communications Manager Administration Configuration Tips

From the Cisco Unified Communications Manager point of view, the trusted relay point (TRP) always gets placed closest to the endpoint device that requires it. The high-level requirements for TRP insertion follow:

- The administrator configures the Use Trusted Relay Point check box in the Common Device Configuration window. The administrator configures the Use Trusted Relay Point drop-down list with On/Off/Default options in the configuration windows of all devices where media terminate, so Cisco Unified Communications Manager knows when to insert a TRP.
- The administrator configures the Trusted Relay Point check box in the MTP Configuration and Transcoder Configuration windows. If you checks this check box when a particular device is configured, Cisco Unified Communications Manager knows that it can use the device as a TRP. The administrator must ensure that a device that is configured as a TRP in Cisco Unified Communications Manager has the appropriate network connectivity and configuration between the TRP and any endpoints that are involved in the call. If the TRP is invoked but does not have the needed connectivity, an audio or video call will not succeed.
- Cisco Unified Communications Manager must insert a TRP for the endpoint if the Use Trusted Relay Point check box is checked for either the endpoint or the device pool that is associated with the device. The call may fail if Cisco Unified Communications Manager fails to allocate a TRP while the Fail Call If Trusted Relay Point Allocation Fails service parameter is set to True.
- If both the MTP Required check box and the Use Trusted Relay Point check box are checked for the endpoint, Cisco Unified Communications Manager should allocate an MTP that is also a TRP. If the administrator fails to allocate such an MTP/TRP, the following table shows the call status, which the values of the Fail Call If Trusted Relay Point Allocation Fails service parameter and the Fail Call if MTP Allocation Fails service parameter also affect.

Fail Call If TRP Allocation Fails	Fail Call If MTP Allocation Fails	Fail Call?
True	True	Yes
True	False	Yes
False	True	Yes, if MTP is required for H.323 endpoint. No, if MTP is required for SIP endpoint.
False	False	No

- If RSVP is enabled for the call, Cisco Unified Communications Manager should first try to allocate an RSVPAgent that is also labeled as TRP. Otherwise, another TRP device gets inserted between the RSVPAgent and the endpoint.
- If a transcoder is needed for the call and needs to be allocated on the same side as the endpoint that needs TRP, Cisco Unified Communications Manager should first try to allocate a transcoder that is also labeled as TRP. Otherwise, another TRP device gets inserted between the transcoder and the endpoint.

- Assuming that both the Fail Call If Trusted Relay Point Allocation Fails service parameter and the Fail Call If MTP Allocation Fails service parameter are set to False, the following table shows the call behavior in relationship to the MTP that is required and Use Trusted Relay Point settings and the resource allocation status.

MTP Required	Use TRP	Resource Allocation Status	Call Behavior
Y	Y	TRP allocated	Audio call only because no pass-through support exists.
Y	Y or N	MTP only	Audio call only. No TRP support.
Y	Y or N	None allocated	If MTP required is checked for H.323 endpoint, supplementary services get disabled.
N	Y	TRP allocated	Audio or video call depends on endpoint capabilities and call admission control (CAC). Supplementary services still work.
N	Y	None allocated	Audio or video call. Supplementary services still work, but no TRP support exists.

- In most instances, TRP gets allocated after users answer the call, so if a call fails due to failure to allocate the TRP, users may receive fast-busy tone after answering the call. (The SIP outbound leg with MTP required, or H.323 outbound faststart, represents an exception.)

GUI Changes

Trusted relay points involve the following new settings in the Cisco Unified Communications Manager Administration GUI:

- **Media Resources > Annunciator**—The Annunciator Configuration window adds the Use Trusted Relay Point setting.
- **Media Resources > Conference Bridge**—The Conference Bridge Configuration window adds the Use Trusted Relay Point setting.
- **Media Resources > Media Termination Point**— The Media Termination Point Configuration window adds the Trusted Relay Point setting.
- **Media Resources > Transcoder**—The Transcoder Configuration window adds the Trusted Relay Point setting.
- **Media Resources > Music On Hold Server**—The Music On Hold Server Configuration window adds the Use Trusted Relay Point setting.
- **Voice Mail > Cisco Voice Mail Port**—The Voice Mail Port Configuration window adds the Use Trusted Relay Point setting.
- **Device > CTI Route Point**—The CTI Route Point Configuration window adds the Use Trusted Relay Point setting.
- **Device > Gateway**—The Gateway Configuration window adds the Use Trusted Relay Point setting.
- **Device > Phone**—The Phone Configuration window adds the Use Trusted Relay Point setting.
- **Device > Trunk**—The Annunciator Configuration window adds the Use Trusted Relay Point setting.

- **Device > Device Settings > Common Device Configuration**—The Common Device Configuration window adds the Use Trusted Relay Point setting.

Service Parameter and Enterprise Parameter Changes

You can configure the Fail Call If Trusted Relay Point Allocation Fails service parameter, which supports the Cisco CallManager service. This service parameter, which is found in the Clusterwide Parameters (System - General) section, determines whether a call that requires a Trusted Relay Point (TRP) is allowed to proceed if no TRP resource is available. Valid values specify True (the call fails if no TRP resource is available) or False (the call proceeds even if a TRP resource is not available).

Choose the best value for a system based on how the system uses TRPs. For example, if the system uses TRP for Virtual Routing and Forwarding (VRF) or for firewall traversal, Cisco Unified Communications Manager cannot connect audio or video without a TRP resource, so the service parameter value should be set to True. If a TRP is used for Quality of Service (QoS) enforcement, Cisco Unified Communications Manager can complete the call if a TRP resource is unavailable, but the call will not have the correct Differentiated Services Code Point (DSCP) marking.

Trusted relay points do not entail any changes to enterprise parameters.

AXL and CTI Considerations

No AXL considerations exist for this feature.

CTI devices, such as CTI route points and CTI ports, can get designated to use a trusted relay point (TRP). These devices can get assigned their own Use Trusted Relay Point setting, or they can inherit their Use Trusted Relay Point setting from their Common Device Configuration setting. The Use Trusted Relay Point setting for an individual device overrides the setting from the associated Common Device Configuration setting.

User Tips

No user tips exist for this feature.

For More Information

- "Media Resource Management," *Cisco Unified Communications Manager System Guide*
- "Media Termination Points," *Cisco Unified Communications Manager System Guide*
- "Transcoders," *Cisco Unified Communications Manager System Guide*
- "Resource Reservation Protocol," *Cisco Unified Communications Manager System Guide*
- "Music On Hold," *Cisco Unified Communications Manager Features and Services Guide*
- "Device Pool Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Annunciator Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Conference Bridge Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Media Termination Point Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Transcoder Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Voice-Mail Port Configuration," *Cisco Unified Communications Manager Administration Guide*
- "CTI Route Point Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Gateway Configuration," *Cisco Unified Communications Manager Administration Guide*

- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Trunk Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Common Device Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Music On Hold," *Cisco Unified Communications Manager Features and Services Guide*

Cisco VG202 and VG204 Gateway Support in Cisco Unified Communications Manager Administration

The Cisco VG202 and VG204 Analog Voice Gateways augment the Cisco Voice Gateway portfolio along with the Cisco Integrated Series Routers (Cisco 3800,2800,1861 and VG224s). These gateways enable an IP telephony solution to continue using traditional analog devices while taking advantage of the productivity that an IP infrastructure affords.

The Cisco VG202 and VG204 comprise Cisco IOS Software-based 2-port and 4-port gateways for analog phones, fax machines, modems, and speakerphones within an enterprise voice system that is based on Cisco Unified Communications Manager and Cisco Unified Communications Manager Express.

After the Cisco VG202 and VG204 release, you can configure the gateways in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration Configuration Tips

No new configuration settings exist in Cisco Unified Communications Manager Administration to support these gateways.

GUI Changes

To configure these gateways in Cisco Unified Communications Manager Administration, choose **Device > Gateway**. Click **Add New** and choose either **VG 202** or **VG 204** from the Gateway Type drop-down list box. After you click **Next**, the Gateway Configuration window displays.

User Tips

These gateways do not impact the end user.

For More Information

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 7.0(1)*.

Voice over Secure IP for SIP Trunks

Voice over Secure IP (VoSIP) for SIP trunks includes the following features:

- Multilevel Precedence and Preemption Enhancements, page 97
- Support for Secure V.150.1 Modem over IP over SIP Trunks, page 98

Note MoIP does not require any configuration in Cisco Unified Communications Manager Administration.

Multilevel Precedence and Preemption Enhancements

This feature adds the following configuration options to Cisco Communications Manager Administration for MLPP: Resource Priority Namespace Network Domain and Resource Priority Namespace Network Domain List. The following sections describe the options.

Resource Priority Namespace Network Domain

The Resource Priority Namespace Network Domain enables the configuration of namespace domains for a Voice over Secured IP (VoSIP) network that uses SIP trunks. Cisco Unified Communication Manager prioritizes the SIP-signaled resources, so those resources can get used most effectively during emergencies and congestion of telephone circuits, IP bandwidth, and gateways. Endpoints receive the precedence and preemption information, which is based on RFC 4411 and RFC 4412.

The SIP signaling contains a resource-priority header. Consider the resource-priority header as similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters that are used in legacy TDM MLPP networks. The resource-priority header relates to, but differs from the priority header in RFC 3261, Section 20.26.

The RFC 3261 priority header indicates the importance of SIP requests for the endpoint. For example, the header could indicate decisions about call routing to mobile devices and assistants and about call acceptance when the call destination is busy. The RFC 3261 priority header does not affect the usage of PSTN gateway or proxy resources.

In the RFC 3261 priority header, any value could get asserted, but the Resource Priority header field in the namespace network domain is subject to authorization. The Resource Priority header field does not directly influence the forwarding behavior of IP routers or the use of communications resources such as packet forwarding priority.

The RFC 4411 and RFC 4412 resource-priority header in the outbound message provides the basis for the translation or route patterns that direct a call to the SIP trunk. Incoming calls get validated against a list of Resource Priority Namespace Network Domains if the calls are terminating that is to an endpoint configured in Cisco Unified Communications Manager Administration.

The following messages include the Resource Priority header:

- INVITE
- UPDATE
- REFER

The following i example shows an INVITE message that has a resource priority header that specifies immediate priority (value of 4).

```
INVITE sip:6000@10.18.154.36:5060 SIP/2.0Via: SIP/2.0/TCP
10.18.154.44;branch=z9hG4bK1636ee4aRemote-Party-ID: "Raleigh - 5001"
<sip:5001@10.18.154.44>;party=calling;screen=yes;privacy=offFrom: "Raleigh - 5001"
<sip:5001@10.18.154.44>;tag=936ad6ec-4d3c-4a42-a812-99ac56d972e1-14875646To:
<sip:6000@10.18.154.36>
Date: Mon, 21 Mar 2005 14:39:21 GMTCall-ID:
1d13800-23e1dc99-4c-2c9a12ac@172.18.154.44Supported: 100rel,timer,replacesRequire:
resource-priorityMin-SE:  1800User-Agent: Cisco-CCM5.0Allow: INVITE, OPTIONS, INFO, BYE,
CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFYCSeq: 101 INVITEContact:
<sip:5001@10.18.154.44:5060;transport=tcp>Expires: 180Allow-Events: presence, dialog,
kpmlCall-Info:<sip:10.18.154.44:5060>;method="NOTIFY;Event=telephone-event;Duration=500"Re
source-Priority: namespace.4
Max-Forwards: 70Content-Type: application/sdpContent-Length: 269v=0o=CiscoSystemsCCM-SIP
2000 1 IN IP4 10.18.154.44s=SIP Callc=IN IP4 10.18.154.45t=0 0m=audio 19580 RTP/AVP 0
101a=rtpmap:0 PCMU/8000a=ptime:20a=rtpmap:101 telephone-event/8000a=fmtp:101 0-15
```

You can also add a default Resource Priority Namespace Network Domain to a SIP profile to use when misconfigured incoming namespace network domains get handled.

Note Digit analysis of translation and route patterns get supported.

The following supplementary services get supported:

- Precedence Call Waiting
- Call Transfer
- Call Forwarding
- Three-way Calling

The following headers, mapping, and queuing do not get supported:

- Accept-Resource-Priority header
- Inclusion of RP header in PRACK and ACK
- Mapping of precedence levels between namespaces
- Call queuing and other non-MLPP services

Resource Priority Namespace Network Domain List

The Resource Priority Namespace Network Domain List contains acceptable network domains and gets added to the SIP profile. Incoming calls get compared to the list and processed if an acceptable network domain is in the list. If the incoming call is not valid, the call gets rejected, and a response of 417 (Unknown) gets sent to the calling party.

Support for Secure V.150.1 Modem over IP over SIP Trunks

This feature adds support for secure V.150.1 based Modem over IP (MoIP) communications between an IP STE and legacy (BRI or analog) STE across interclustered SIP trunks. SIP trunks transport the Session Description Protocol (SDP) information for outbound calls and signal Cisco Unified Communications Manager when MoIP SDP information is received for inbound calls. Devices can call between clusters by using SIP to negotiate a V.150.1 secure call.

Note No additional configuration tasks for this feature exist.

Cisco Unified Communications Manager Administration Configuration Tips

No Cisco Unified Communications Manager Administration configuration tips exist for these features.

GUI Changes

The following GUI changes occurred for this feature.

- To configure a Resource Priority Namespace Network Domain and enable secure MLPP for SIP trunks, choose **System > MLPP > Namespace > Resource Priority Namespace Network Domain**.
- To configure a list of Resource Priority Namespace Network Domains, choose **System > MLPP > Namespace > Resource Priority Namespace Network Domain List**.
- To configure the translation pattern for a Resource Priority Namespace Network Domain, choose **Call Routing > Translation Pattern**.
- To configure a SIP profile for a device, choose **Device > Device Settings > SIP Profile**.

- To configure a SIP trunk for secure MLPP, choose **Device > Trunk**.

User Tips

No software, hardware, or firmware restrictions exist. No accessibility restrictions or special configuration considerations exist.

For More Information

Refer to the following documents for additional configuration details for this feature:

- *Cisco Unified Communications Manager Features and Services Guide, Release 7.0(1)*
- *Cisco Unified Communications Manager Administration Guide, Release 7.0(1)*
- *Cisco Unified Communications Manager System Guide, Release 7.0(1)*

Bulk Administration Tool

This section contains information on the following topics:

- Time of Day Access feature for the Bulk Administration Tool, page 99
- Import and Export Enhancements for the Bulk Administration Tool, page 100
- TAPS Name Change in Bulk Administration Tool, page 103

Time of Day Access feature for the Bulk Administration Tool

You can insert, delete, and export Time of Day Access by using the Time of the Day Access menu in the Bulk Administration Tool:

- Inserting Time of Day Access, page 99
- Deleting Time of Day Access, page 99
- Exporting Time of Day Access, page 99

Inserting Time of Day Access

You can insert Time of Day Access through Bulk Administration Tool. You can access the Time of Day Access Insert window by choosing **Bulk Administration > Mobility > Time of Day Access Insert**.

Deleting Time of Day Access

You can delete Time of Day Access through Bulk Administration Tool. You can access the Time of Day Access Delete window by choosing **Bulk Administration > Mobility > Time of Day Access Delete**.

Exporting Time of Day Access

You can export Time of Day Access through Bulk Administration Tool. You can access the Time of Day Access Export window by choosing **Bulk Administration > Mobility > Time of Day Access Export**.

GUI Changes

The following changes occurred in the GUI of the Mobility submenu:

- Bulk Administration > Mobility > Time of Day Access Insert
- Bulk Administration > Mobility > Time of Day Access Delete
- Bulk Administration > Mobility > Time of Day Access Export

For More Information

For information on Time of Day features in BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*, *Release 7.0(1)*.

Import and Export Enhancements for the Bulk Administration Tool

The Import/Export tool in BAT includes new updates to support the export of Cisco Unified Communications Manager configuration details. It also has a new feature to validate .tar import files.

GUI Changes

The following changes occurred in the GUI of the Import/Export submenu:

- Exporting Configuration, page 100
- Validate Import File, page 103

Exporting Configuration

You can use BAT to export many new items in Release 7.0. The following list gives check boxes that are now available on the Export Configuration window for you to choose:

System Data

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Group
- Date/Time Group
- Device Pool
- Enterprise Parameter
- Location
- Phone NTP Reference
- Region
- Server
- Service Parameter
- SRST
- Security Profile (Phone & SIP Trunk)
- Physical Location
- Device Mobility group
- Presence Group
- LDAP System
- Device Mobility Info
- DHCP Server
- DHCP Subnet

- Application Server
- LDAP Directory
- LDAP Authentication
- MLPP Domain
- Resource Priority Namespace Network Domain
- Resource Priority Namespace List
- CUMA Server Security Profile

Call Routing Data

- Application Dial Rules
- CSS (Class of Control)
- Partitions (Class of Control)
- Route Filter
- Time Period (Class of Control)
- Time Schedule (Class of Control)
- Translation Pattern
- AAR Group
- Forced Authorization Codes
- Directory Lookup Dial Rules
- Client Matter Codes
- Call Park
- Call Pickup Group
- Directory Number
- MeetMe Number
- Cisco Attendant Console Pilot Point
- Directed Call Park
- SIP Dial Rules
- Line Group
- Route Group
- Hunt List
- Route List
- Hunt Pilot
- Intercom Route Partition
- Intercom CSS
- Access List
- Route Pattern
- Called Party Transformation Pattern
- SIP Route Pattern
- Intercom Directory Number

- Mobility Configuration
- Intercom Translation Pattern
- Calling Party Transformation Pattern
- Time Of Day Access

Media Resources

- Annunciator
- Conference Bridge
- Media Resource Group
- Media Resource Group List
- Media Termination Point
- Transcoder
- MOH Server
- Mobile Voice Access

User Data

- SIP Realm
- Application User
- User Group
- Role
- Application User CAPF Profile
- Credential Policy Default
- Credential Policy
- End User
- End User CAPF Profile
- Cisco Attendant Console User

Device Data

- Softkey Template
- Gate Keeper
- Trunk
- SIP Profile
- Phone Services
- Phone Button Template
- Common Phone Profile
- Gateway
- Device Defaults
- Device Profile
- Common Device Configuration
- CTI Route Point
- Phone

- Recording Profile
- Remote Destination
- Remote Destination Profile

Voice Mail Data

- Message Waiting Numbers
- Voice Mail Pilot
- Voice Mail Profile
- Voice Mail Port

You can access the Export Configuration window by choosing **Bulk Administration > Import/Export > Export.**

Validate Import File

You can use the Validate Import File window in BAT to validate the import .tar file. You can use this feature to validate the following items:

- The .tar file includes a header file.
- All files that are listed in the header file actually exist in the .tar file.
- All files in the .tar file get listed in header file.
- File names specify correct file names(as per the Import/Export convention).
- File format for the CSV files in the .tar file specifies a correct format.

Note This feature does not include field level validation for valid characters, string length, and so on.

You can access this feature by choosing **Bulk Administration > Import/Export > Validate Import File**.

For More Information

For information on configuring additional features in BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*, *Release 7.0*.

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. You should read all references to 'Cisco Unified Communications Manager Auto-Register Phone Tool' in the Bulk Administration Tool Online Help as 'Tool for Auto-Registered Phone Support (TAPS)'. This makes it in compliance with the Bulk Administration user interface.

For More Information

For information on configuring additional features in BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*, *Release 7.0*.

Security

The following security enhancements exist for Cisco Unified Communications Manager Release 7.0:

Cisco Unified Mobility Advantage Server Security Profile

Cisco Unified Communications Manager Administration groups security-related settings to allow you to assign a single security profile to multiple Cisco Unified Mobile Communicator clients. Security-related settings include device security mode, incoming transport type, and X.509 subject name. Configuring a Cisco Unified Mobility Advantage server security profile in Cisco Unified Communications Manager Administration automatically applies this profile to all configured Cisco Unified Mobility Communicator clients on that Cisco Unified Communications Manager.

Only the security features that the Cisco Unified Mobility Advantage server supports display in the security profile settings window.

Note You cannot configure Cisco Unified Mobility Advantage servers in Cisco Unified Communications Manager Administration. For information on setting up a security profile for a Cisco Unified Mobility Advantage server, refer to your Cisco Unified Mobility Advantage documentation. Make sure that the Cisco Unified Mobility Advantageh Security Profile that you configure on Cisco Unified Communications Manager matches the security profile on the Cisco Unified Mobility Advantage servers. For information on configuring a Cisco Unity Mobility Advantage server security profile, refer to the *Cisco Unified Communications Manager Security Guide*.

GUI Changes

In Cisco Unified Communications Manager Administration, choose **System > Security Profile > CUMA Server Security Profile**.

The Find and List CUMA Server Security Profile window displays. Records from an active (prior) query may also display in the window. From this window, you can search for an existing Cisco Unified Mobility Advantage Server profile and then edit that profile if desired, or you can click **Add New** to configure a new Cisco Unified Mobility Advantage Server profile.

Configuration Tips

You cannot delete a security profile that is currently assigned to a Cisco Unified Mobile Communicator client.

If you change the settings in a security profile that is already assigned to a Cisco Unified Mobile Communicator client, the reconfigured settings apply to all Cisco Unified Mobile Communicator clients that are assigned that profile.

You can rename security files that are assigned to Cisco Unified Mobile Communicator clients. The Cisco Unified Mobile Communicator clients that are assigned the old profile name and settings assume the new profile name and settings.

For More Information

Refer to the *Cisco Unified Communications Manager Security Guide*.

Secure-Indication Tone Configuration

The secure-indication tone represents a special tone that gets played on both ends of a call that is established through devices that are configured as "protected" and when encrypted media is established. The tone denotes that the call is protected and that confidential information may get exchanged. The tone lasts for 2 seconds and begins to play as soon as the called party answers.

A "protected" device in Cisco Unified Communications Manager gets designated by configuration. Only certain Cisco Unified IP Phones and MGCP E1 PRI gateways can get configured as protected devices in Cisco Unified Communications Manager.

Therefore, the following two types of calls that can use the secure-indication-tone feature can be made:

- Intracluster IP-to-IP calls
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI Gateway

Configuration Requirements

You must configure the following items for the secure tone to play:

- In the Phone Configuration window, to which you can navigate by choosing **Device > Phone** in Cisco Unified Communications Manager Administration, configure the following items:
  - From the Softkey Template drop-down list in the Device Information portion of the window, choose **Standard Protected Phone**.

Note You must use a new softkey template without supplementary service softkeys for a protected phone.

  - For the Join Across Lines option (also in the Device Information portion of the window), choose **Off**.
  - Check the **Protected Device** check box (also in the Device Information portion of the window).
  - From the Device Security Profile drop-down list (in the Protocol Specific Information portion of the window), choose a secure phone profile that has already been configured in the Phone Security Profile window (**System > Security Profile > Phone Security Profile**).
- Go to the Directory Number Configuration window that displays when you add a directory number from the Phone Configuration window. In the portion of the Directory Configuration window that is called Multiple Call/Call Waiting Settings on Device DeviceName, set the following options to a value of 1:
  - Maximum Number of Calls
  - Busy Trigger
- Choose **System > Service Parameters** in Cisco Unified Communications Manager Administration, select your server, and select the Cisco CallManager service. On the Service Parameter Configuration window, in the Feature - Secure Tone portion, set the Play Secure Indication Tone option to **True** (default specifies False).
- If you are configuring a protected MGCP E1 PRI gateway, choose **Device > Gateway > Add New** in Cisco Unified Communications Manager Administration and select a supported gateway. (The "Secure-Indication Tone" chapter in the *Cisco Unified Communications Manager Security Guide*. lists the supported gateways.) Select MCGP as the protocol. When the Gateway Configuration window displays, be sure to include the following configuration choices:
  - Set Global ISDN Switch Type to **Euro**.

– After you complete the rest of the MGCP Gateway configuration, click **Save**; then, select the endpoint icon that displays to the right of subunit 0 in the window. The **Enable Protected Facility IE** check box displays. Check this check box.

  This allows the passing of protected status between Cisco Unified IP Phone endpoints and the protected PBX phones that are connected to the MGCP gateway.

For More Information

Refer to the *Cisco Unified Communications Manager Security Guide*, "Secure-Indication Tone" chapter.

SIP Trunk SRTP

A SIP trunk will report encrypted or not-authenticated security status when the TLS transport type is used. When SRTP is negotiated, the security status gets encrypted; otherwise, it will be not-authenticated. This will allow Cisco Unified Communications Manager call control to determine the overall security level of a call that involves a SIP trunk. Existing signals to Cisco Unified Communications Manager call control that are used for other device types also get used by a SIP trunk.

GUI changes

In Cisco Unified Communications Manager Administration, choose **Device > Trunk > SIP Trunk Configuration** and locate the check box **SRTP Allowed**.

Check this check box if you want Cisco Unified Communications Manager to allow secure and nonsecure media calls over the trunk. Checking this check box enables Secure Real-Time Protocol (SRTP) over encrypted TLS SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP.

If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP negotiation instead.

The default value for this check box leaves it unchecked.

Caution If you check this check box, you must configure the SIP trunk to use TLS, so keys and other security-related information do not get exposed during call negotiations. If you do not configure TLS correctly, SRTP will not work.

For More Information

Refer to the following documents:

- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Administration Guide*, Trunk Configuration chapter, "Trunk Configuration Settings for SIP Trunks" table

Cisco Unified Serviceability

This section contains these subsections:

New Enterprise Parameters for Alarm Configuration

Cisco Syslog Agent enterprise parameters in Cisco Unified Communications Manager Administration allow you to forward all alarms that meet or exceed the configured threshold to a remote syslog server with these two settings: remote syslog server name and syslog severity. The alarms include system (OS/hardware platform), application (services), and security alarms. If you have a Cisco Unified Communications Manager Business Edition server, the system also forwards Connection alarms.

To access the Cisco Syslog Agent parameters, choose **System > Enterprise Parameters** in Cisco Unified Communications Manager Administration and configure the remote syslog server name and syslog severity; then, click **Save**. For the valid values to enter, click the **?** button. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Note Do not configure a Cisco Unified Communications Manager as a remote syslog server. The Cisco Unified Communications Manager server does not accept Syslog messages from another server.

Note If you configure both the Cisco Syslog Agent alarm enterprise parameters and application (service) alarms in Cisco Unified Serviceability, the system can send the same alarm to the remote syslog twice.

If local syslog is enabled for an application alarm, the system sends the alarm to the enterprise remote syslog server only when the alarm exceeds both the local syslog threshold and the enterprise threshold If remote syslog is also enabled in Cisco Unified Serviceability, the system forwards the alarm to the remote syslog server by using the application threshold that is configured in Cisco Unified Serviceability, which may result in the alarm getting sent to the remote syslog server twice.

Configuring the Application Billing Servers

When you configure the application billing servers, two new billing application server parameters exist:

- Resend on Failure—When you check the **Resend on Failure** check box, this option informs the CDR Repository Manager (CDRM) not to send outdated CDR and CMR files to the billing server after the FTP or SFTP connection is restored. When the check box is checked, the Resend on Failure flag gets set to True. When the check box is not checked, the Resend on Failure flag gets set to False
- Generate New Key—Click the **Reset** button to generate new keys and reset the connection to the SFTP server.

Vendor-Supported MIB OIDs and Descriptions Now Available

Find the Object IDs (OIDs) for vendor-supported MIBS and their descriptions in the *Vendor MIB Support for Cisco Unified Communications Manager Servers* document at this location:

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

Cisco Unified Real-Time Monitoring Tool

This section contains these subsections:

Four Perfmon Counters Added

This section contains information about the four new counters.

CM_MediaTermPointsRequestsThrottled

The CM_MediaTermPointsRequestsThrottled counter represents the total number of media termination point (MTP) resource requests that have been denied due to throttling (a resource from this MTP did not get allocated because, as specified by the Cisco CallManager service parameter, MTP and Transcoder Resource Throttling Percentage, the MTP was being utilized beyond the configured throttle percentage.)

This counter increments each time that a request for an MTP on this Cisco Unified Communications Manager (Cisco Unified CM) is requested and denied due to MTP throttling and reflects a running total since the start of the Cisco CallManager service.

CM_TranscoderRequestsThrottled

The CM_TranscoderRequestsThrottled counter represents the total number of transcoder resource requests that have been denied due to throttling (a resource from this transcoder did not get allocated because, as specified by the Cisco CallManager service parameter, MTP and Transcoder Resource Throttling Percentage, the transcoder was being utilized beyond the configured throttle percentage.)

This counter increments each time that a request for a transcoder on this Cisco Unified Communications Manager (Cisco Unified CM) is requested and denied due to transcoder throttling and reflects a running total since the start of the Cisco CallManager service.

MTP_RequestsThrottled

The MTP_RequestsThrottled counter represents the total number of media termination point (MTP) resource requests that have been denied due to throttling (a resource from this MTP did not get allocated because, as specified by the Cisco CallManager service parameter, MTP and Transcoder Resource Throttling Percentage, the MTP was being utilized beyond the configured throttle percentage.)

This counter increments each time that a resource is requested from this MTP and is denied due to throttling. This counter reflects a running total since the MTP device registered with the Cisco CallManager service.

XCODE_RequestsThrottled

The XCODE_RequestsThrottled represents the total number of transcoder resource requests that have been denied due to throttling (a resource from this transcoder was not allocated because, as specified by the Cisco CallManager service parameter, MTP and Transcoder Resource Throttling Percentage, the transcoder was being utilized beyond the configured throttle percentage.)

This counter increments each time a resource is requested from this transcoder and is denied due to throttling. This counter reflects a running total since the transcoder device registered with the Cisco CallManager service.

New Preconfigured Perfmons

This release adds the following new system performance-monitoring Memory counters:

Note The RisDC Perfmon Log counter adds Low Total and Low Free counters to .csv file counter selections.

Table 6 System Performance-Monitoring Memory Counters

Faults Per Sec	This counter represents the number of page faults (both major and minor) that the system made per second (post 2.5 kernels only). This does not necessarily represent a count of page faults that generate I/O because some page faults can get resolved without I/O.
Low Total	This counter represents the total low (non-paged) memory for kernel.
Low Free	This counter represents the total free low (non-paged) memory for kernel.
Major Faults Per Sec	This counter represents the number of major faults that the system made per second that have required loading a memory page from disk (post 2.5 kernels only).
Pages Input Per Sec	This counter represents the total number of kilobytes that the system paged in from the disk per second.
Pages Output Per Sec	This counter represents the total number of kilobytes that the system paged out to the disk per second.

This release adds the following new system performance-monitoring Process counter:

Table 7 System Performance Monitoring Process Counter

Wchan	This counter displays the channel (system call) in which the process is waiting.

CTIManager Improved Throughput

If more than one logical disk drive is available in your system, Cisco Unified Communications Manager stores CTIManager traces in the ‘spare’ partition on the first logical disk and Cisco CallManager traces on the second logical disk. RTMT monitors the disk usage for the “spare” partition in the Disk Usage window.

You cannot add partitions during the upgrade process. To obtain the throughput benefits for CTIManager, you must back up the existing system, complete a fresh install to release 6.0(1) or later, and restore the configuration.

The following new alarms, counters, and alerts support the spare partition:

- System LpmTct Catalog Alarms:

  - SparePartitionLowWaterMarkExceeded—The percentage of used disk space in the spare partition exceeded the configured low water mark. Severity equals ERROR_ALARM.
  - SparePartitionHighWaterMarkExceeded—The percentage of used disk space in the spare partition exceeded the configured high water mark. Severity equals ERROR_ALARM.
- Preconfigured System Disk Usage Perfmons: Spare Partition Usage—The disk usage monitoring category displays the percentage of disk usage for the Spare partition in each host.
- Preconfigured System Alerts
  - SparePartitionHighWaterMarkExceeded—This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table 8 Default Configuration for the SparePartitionHighWaterMarkExceeded

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert occurs when following condition is met: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

  - SparePartitionLowWaterMarkExceeded: This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds equals less than the low water mark.

Default Configuration

Table 9 Default Configuration for the SparePartitionLowWaterMarkExceeded

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert occurs when following condition is met: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)

Table 9 Default Configuration for the SparePartitionLowWaterMarkExceeded

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Simultaneous Alert Configuration

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* adds a procedure that describes how to use the "Default" alert action to configure settings for all precanned alerts at once.

All precanned alerts initially get assigned the Default alert action. The Default alert action configures the alerts for syslog and alert logging. When you add e-mail destinations to the Default alert action, all precanned alerts get sent to those recipients (provided the alerts continue to use the Default alert action). Updating the Default alert action impacts all alerts that you configured with the Default alert action. You cannot remove the "Default" alert action.

Note To customize a specific alert, you use the Set Alerts/Properties option, which displays when you right-click an alert in Alert Central.

Procedure

Step 1 In the QuickLaunch Channel, click **Alert Central**.

The Alert Central window displays.

Step 2 Click **System > Tools > Alert > Config Alert Action**.

The Alert Action box displays.

Step 3 In the Alert Action list, select Default (highlight the item) and click **Edit**.

The Action Configuration box displays.

Step 4 (Optional) Enter a description of the default list.

Step 5 To add a recipient, click **Add**. The Input box displays.

Step 6 Enter an e-mail destination for the alerts. Click **OK**.

The e-mail address displays in the Recipients list in the Action Configuration box.

Note When you add a recipient, e-mail notifications to that destination get enabled by default. To disable e-mail notifications to a destination, uncheck the check box next to the destination in the Enable column. To disable all e-mails for a specific alert, use the Set Alerts/Properties settings for the alert and deselect Enable Email.

Step 7 Return to Step 5 to add more e-mail destinations, as required.

Note To completely remove a recipient, highlight the recipient in the list and click **Delete**.

RTMT Alert Help in Syslog Viewer

CiscoSyslog messages now display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

Alert Definitions and Defaults

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* adds these new appendixes:

- Appendix D: System Alert Descriptions and Default Configurations
- Appendix E: CallManager Alert Descriptions and Default Configurations
- Appendix F: Cisco Unity Connection Alert Descriptions and Default Configurations (for Cisco Unified CM Business Edition only)

Cisco Unified Communications Manager CDR Analysis and Reporting

This section contains these subsections:

- Configuring CDR Search by Cause for Call Termination, page 117
- Enabling or Customizing Reports for Automatic Generation, page 117

CAR Documentation Omits Information on Up and Down Arrows

The "Configuring Bills User Reports" chapter in the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide* does not state the purpose of the up and down arrows when you configure department bill reports. Use the following information for Step 6 when you configure the department bill reports in the Department Bills window.

Step 6. To choose all of your direct reports in the Department Bills window, check the **Select All Reportees** check box. The List of Reportees shows your direct reports.

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

CAR Administrator Privileges Disappear after an Upgrade is Accomplished by Using DMA

When you use Data Migration Assistant (DMA) to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade. The CAR users become standard end users. You must reset the CAR administrator privileges after the upgrade.

For More Information

"Configuring CAR Administrators, Managers, and Users" section in the *CDR Analysis and Reporting Administration Guide*.

Cisco Call Detail Records Has New Guide

With this release, you find information about Cisco Call Detail Records (CDRs) in the *Cisco Unified Communications Manager Call Detail Records Administration Guide*. The *CDR Analysis and Reporting Administration Guide* no longer includes CDR information.

Upgrading Cisco Unified Communications Manager

When you upgrade from an earlier version of Cisco Unified Communications Manager to a later version of Cisco Unified Communications Manager, you may find that you cannot upgrade all your CDR data.

Backup of CAR Database

The CAR and CDR Disaster Recovery Service (DRS) now integrates into the Disaster Recovery System (DRS). The DRS includes the backup of the CAR database, pregenerated reports, and the CDR preserved flat files.

CPU Utilization

Cisco performed basic testing to measure CPU utilization when CDRs and/or CMRs are enabled. Table 2-1 in the *CDR Analysis and Reporting Administration Guide* displays the results of these tests.

New CDR Service Parameters

To access the Service Parameters Configuration window, open Cisco Unified Communications Manager Administration and choose **System -> Service Parameters**. Choose the **Advanced** button to display the complete list of Service Parameters. The following new service parameters can affect CDR/CMR records:

- **Show Line Group Member DN in finalCalledPartyNumber CDR Field**—This parameter determines whether the finalCalledPartyNumber field in CDRs shows the directory number (DN) of the line group member who answered the call or the hunt pilot DN. Valid values specify True (the finalCalledPartyNumber in CDRs will show the DN of the phone that answered the call) or False (the finalCalledPartyNumber in CDRs will show the hunt pilot DN). This parameter applies only to basic calls that are routed through a hunt list without feature interaction such as transfer, conference, call park, and so on. If a feature is involved in the call, the hunt pilot DN will show in the finalCalledPartyNumber field regardless of the setting in this parameter. This parameter does not apply to Cisco Unified Communications Manager Attendant Console. The default value for this required field specifies False.
- **Add Incoming Number Prefix to CDR** —This parameter determines whether Cisco Unified Communications Manager adds the incoming prefix (as specified in the National Number Prefix, International Number Prefix, Subscriber Number Prefix, and Unknown Number Prefix service parameters) to the calling party number in the CDRs for that call. If the prefix is applied on the inbound side of the call, it will always get added to the calling party number in the CDRs for that call, even if this parameter is set to False. If the prefix is applied on the outbound side, the prefix will get added to the calling party number in the CDR(s) for that call only if this parameter is set to True. If the destination of the call is a gateway, Cisco Unified Communications Manager will not add the prefix to the CDRs even if this parameter is enabled. This parameter also applies clusterwide. The default value for this required field specifies False.
- **Use Global Call ID of Parked Call Enabled**—This parameter determines whether the globalCallId that is reported in call detail records (CDRs) and Cisco Unified JTAPI applications changes to a new globalCallId when a call gets retrieved from park. This service parameter determines whether Cisco Unified Communications Manager preserves the globalCallId of parked calls or perpetuates the new globalCallId when the call is retrieved from park. Valid values specify True (when the call is retrieved from park, Cisco Unified Communications Manager preserves the original globalCallId that was associated with the parked call) or False (Cisco Unified Communications Manager creates a new globalCallId when the call gets retrieved from park). Choosing True makes it easier to correlate CDR data because the same globalCallId gets retained for the duration of the call; however, some CTI applications may see a change in behavior for globalCallId event reporting. Enable this parameter when backwards compatibility issues with CTI applications exists. The default value for this field specifies False.

Logging On to CAR

Only CAR administrators and normal end users can log on to the CAR web interface. Users do not need to be a member of a standard CAR administrator group to be a CAR administrator. Any user who has the role, Standard Admin Rep Tool Admin, associated with the user ID can access CAR as a CAR administrator. The user ID role association gets done by adding the user to a user group that has the role associated with it. Standard CAR Admin Group and Standard CCM Super Users comprise two groups that have the role, Standard Admin Rep Tool Admin, associated with them. The default application user that gets created at installation, who is a member of the Standard CCM Super Users group, can log in to CAR as a CAR administrator but only as an application user. This user cannot access the Individual Bills report.

Supported Versions of FTP/SFTP for Billing Servers

The CDR Repository Manager sends CDR files to up to three preconfigured destinations (billing servers) that are using FTP/SFTP. Make sure that your billing server uses one of the following versions of FTP or SFTP that Cisco tested and supports:

- Linux/Unix
  - FTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)
  - SFTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)
- Windows
  - FTP: Microsoft FTP service (Windows 2000 5.00.2195 sp4, IIS 5.0) and WAR FTP Daemon (1.82.0.10) and FreeFTPd (1.0.10 and 1.0.11)
  - SFTP: FreeFTPd (1.0.10 and 1.0.11)

Configuring Individual and Department Bills Reports

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

Procedure for Adding Owner User ID to Individual Bills

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

Add the information for the device and the user.

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

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

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

Add the information for the device and the user.

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

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

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

reports for a particular end user in the directory, either the User ID for the particular end user must be configured as the Owner User ID for the device or the particular end user must have logged in to the device with the Cisco Extension Mobility feature enabled.

Configuring CDR Error Reports

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

Table 16-1 in the *CDR Analysis and Reporting Administration Guide* lists the CDR error codes and the definition of the error.

Configuring Mail Server Parameters

You must use additional information to configure the mail server parameters.

In the CAR window, go to **System > System Parameters > Mail Parameters**. In the Mail ID field, only enter the e-mail identifier that will get used in the From field when e-mails are sent (for example, smith1@abc.com, enter **smith1** in the Mail ID field).

In the Mail Server Name field, enter the domain name for the server that runs the e-mail system (that is **abc.com** from the preceding example).

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

Configuring the CDR Load Schedule

The default batch size specifies 600 CDR or CMR. The default sleep time between each CDR batch equals 2500 ms and 3000 ms for each CMR batch. However, you can configure the batch size from the tbl_system_preferences table “Loader Batch” column to have any value between 50 and 2000.

Manual Purging or Reloading the CAR Database

Manual purging of the CDRs stops if the CAR Web Service is stopped during the manual purge process. Manual purging cannot begin again until the CAR Web Service restarts. Then, you must begin the manual purge process again.

You can perform the following tasks to intentionally stop the CAR Web Service:

- Deactivate the CAR Web Service in the Serviceability Service Activation window (**Cisco Unified Serviceability > Service Activation**).
- Stop the CAR Web Service in the Feature Services window of the Serviceability Control Center (**Cisco Unified Serviceability > Tools > Control Center - Feature Services**).

The CDR Loader cannot begin again until either the CAR Web Service or the CAR Scheduler gets restarted.

Generating the CAR System Event Log

This release of Cisco Unified Communications Manager introduces the The Task Monitor and Database Maintenance features.

Task Monitor begins about 1 minute after the Scheduler starts, and 1 minute after the Scheduler repopulates the schedules every day at midnight (00.00). The Task Monitor periodically (every 5 minutes) monitors the status of all jobs for the day from the tbl_event_log with the exception of the following jobs: PopulateSchedules, TaskMonitor, DatabaseMaintenance, and DailyCdrLoad.

When a task does not start on schedule because an earlier task is still running, you may see something like the following trace message:

```
2008-02-14 08:00:04, 602 WARN [main] services. Scheduler - runTasks(): Job [DailyCdrLoad]
thread is busy, hence it will be removed from today's schedule and not be started!"
```

The Scheduler gives a grace period to periodically sleep for 10 seconds and check whether the task thread is complete. The Scheduler sleeps up to 2 minutes total. If the task thread does not complete after the 2 minutes of wait time, the next task gets removed from the current schedule and does not run until its next scheduled time.

Event Log Report Status

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

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

CAR Alarm Catalog

This release of Cisco Unified Communications Manager introduces a CAR alarm catalog (CARAlarmCatalog.xml) for the CAR Scheduler. Table 29-3 in the *CDR Analysis and Reporting Administration Guide* displays the alarms/alerts in this catalog.

Upgrading the CAR Database

When you upgrade the CAR database from Cisco Unified Communications Manager Release 4.x to Release 5.x, 6.x, or 7.x, the Cisco Unified Communications Manager installation program limits the time for the migration of the CAR records from the CSV files in the Data Migration Assistant (DMA) TAR file to the CAR database on the upgraded system. The migration time specifies 60 minutes. Review this information to determine how to migrate the highest number of CSV files in the allotted time.

Configuring CDR Search by Cause for Call Termination

Only CAR administrators use the CDR Search by Cause for Call Termination feature. Table 25-1 in the *CDR Analysis and Reporting Administration Guide* includes new call termination cause codes by which you may search.

Enabling or Customizing Reports for Automatic Generation

For all new installations of Cisco Unified Communications Manager, you must first enable the e-mail alerts and reports for automatic generation. The default status for all reports and alerts specifies **Disabled**.

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.

Cisco Unified Communications Manager Call Detail Records

This section contains these subsections:

Global Call Identifier

The Cisco Unified Communications Manager allocates a global call identifier (GlobalCallID_callId) each time that a Cisco Unified IP Phone is taken off hook or a call is received from a gateway. The GlobalCallID_callId gets allocated sequentially on a Cisco Unified Communications Manager server. Cisco Unified Communications Manager writes the GlobalCallID_callId value to a disk file for every 1,000th call. When Cisco Unified Communications Manager restarts for any reason, it assigns the next 1000th number to the next GlobalCallID_callId.

Partition/Extension Numbers in CDRs

The following new partition/extension numbers fields exist in the CDR record:

- outpulsedCallingPartyNumber—The calling party number outpulsed from the device.
- outpulsedCalledPartyNumber—The called party number outpulsed from the device.

Calling Party Normalization and Support for Dialing “+”

Cisco Unified Communications Manager supports the new feature, Calling Party Normalization and support for dialing “+”, in this release. The callingPartyNumber, originalCalledPartyNumber, finalCalledPartyNumber, lastRedirectDN, and the new fields, outpulsedCallingPartyNumber and outpulsedCalledPartyNumber can now contain a “+” in the CDR. The device reports the calling party number that it outpulses to call control only if calling party normalization/localization takes place. This information gets recorded in the CDR in the outpulsedCallingPartyNumber field. CDR examples exist for Calling Party Normalization and “+” dialing.

Local Route Groups and Called Party Transformation

In this release, Cisco Unified Communications Manager supports the new feature, local route groups and called party transformation. CDR examples exist for the **outpulsedCalledPartyNumber** and the **outpulsedCallingPartyNumber** fields.

Call Park CDR Examples with the Use Global Call ID of Parked Call Service Parameter

The useGcidOfParkedCallEnabled service parameter gets introduced in this release of Cisco Unified Communications Manager. The default value of False provides that, when the call is retrieved from park Cisco Unified Communications Manager creates a new globalCallId. The value of True provides that, when the call is retrieved from park, Cisco Unified Communications Manager retains the original globalCallId. The following CDRs display these scenarios.

Call Park Pickup with GcidOfParkedCallEnabled Service Parameter Set to False CDR Example

50003 calls 50002; 50002 presses the Park softkey. 50001 picks up the parked call by dialing the park code (44444).

Field Names	Original Call That Is Parked CDR	Parked Call That Is Picked Up CDR
globalCallID_callId	1	2
origLegCallIdentifier	20863957	20863961
destLegCallIdentifier	20863958	20863957
callingPartyNumber	50003	50001
originalCalledPartyNumber	50002	50003
finalCalledPartyNumber	50002	50003
lastRedirectDn	50002	44444
origCause_Value	393216	0
dest_CauseValue	393216	16
origCalledPartyRedirectReason	0	0
lastRedirectRedirectReason	0	8
origCalledPartyRedirectOnBehalfOf	0	0
lastRedirectRedirectOnBehalfOf	0	3
origTerminationOnBehalfOf	3	0
destTerminationOnBehalfOf	3	12
joinOnBehalfOf	0	3
duration	4	60

Call Park Pickup with GcidOfParkedCallEnabled Service Parameter Set to True CDR Example

50003 calls 50002; 50002 presses the Park softkey. 50001 picks up the parked call by dialing the park code (44444).

Field Names	Original Call That Is Parked CDR	Parked Call That Is Picked Up CDR
globalCallID_callId	1	1
origLegCallIdentifier	20863957	20863961
destLegCallIdentifier	20863958	20863957

callingPartyNumber	50003	50001
originalCalledPartyNumber	50002	50003
finalCalledPartyNumber	50002	50003
lastRedirectDn	50002	44444
origCause_Value	393216	0
dest_CauseValue	393216	16
origCalledPartyRedirectReason	0	0
lastRedirectRedirectReason	0	8
origCalledPartyRedirectOnBehalfOf	0	0
lastRedirectRedirectOnBehalfOf	0	3
origTerminationOnBehalfOf	3	0
destTerminationOnBehalfOf	3	12
joinOnBehalfOf	0	3
duration	4	60

Video Conference Call CDR Example

An example of a video conference call gets added to the CDR examples.

New CDR Field Descriptions

The **outpulsedCalledPartyNumber** and the **outpulsedCallingPartyNumber** fields get added to the CDR field descriptions as new fields.

Cisco-Specific Call Termination Cause Codes

The Cisco-Specific call termination cause codes table in Table 6-3 of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* presents both decimal value codes and hex value codes.

Cisco Devices That Support VarQMetrics

Table 9-2 of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* displays a list of all Cisco devices that support varQMetric information in the call management records (CMRs).

CMR Example

The documentation now provides an example of a typical CMR.

Cisco Unified Reporting

Cisco Unified Reporting includes new report data that is now available. Trace settings for the 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*.

Cisco Unified JTAPI Developers Guide

The following sections describe the new and changed features and enhancements to the *Cisco JTAPI Developers Guide for Cisco Unified Communications Manager Release 7.0(1)*:

Note Be aware that IPv6 is not supported.

For interface and message sequence changes, refer to the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager Release 7.0(1)*.

Join Across Lines with Conference Enhancements

The Join Across Lines with Conference enhancements follow:

- Conference chaining across lines; for example, applications can conference two conference calls in which each conference exists on a different address but on the same terminal.
- Add participants to a conference by using a noncontroller.

Locale Infrastructure Development

This feature removes currently supported languages for JTAPI client install. JTAPI client install only gets supported in English. It also adds the capability to dynamically update the locale in JTAPI Preference application from the Cisco Unified Communications Manager server. JTAPI Preference application will continue to support all the languages that are supported in prior releases. This release also adds support for adding new languages and updating locale files .

This feature adds the capability to dynamically update locale file for JTAPI Preferences application, and you can install JTAPI Client only in English languages.

The JTAPI Client install needs the Cisco Unified Communications Manager TFTP server IPaddress. The TFTP IP address gets used for downloading locale files for the preferences application. If the TFTP IP address is not entered or an incorrect IP address is entered, the preference application displays only in English language.

Backward Compatibility

From the JTAPI application perspective, consider this a backward compatible feature, but from the JTAPI client install perspective, because currently supported languages have been removed, do not consider it as a backward compatible feature.

Do Not Disturb–Reject

Do Not Disturb–Reject (DND–R) represents an enhancement to the existing DND feature. Cisco Unified Communications Manager and JTAPI previously supported only the Ringer off DND. The user can reject calls with DND–Reject. You can set DND–R from phone configuration or the phone profile configuration window in Cisco Unified Communications Manager Administration.

When DND–R is enabled, the call does not get presented to the terminal that has Call Reject enabled. No audible or visual indication of incoming calls on that end point occurs. To enable DND–R, set the DND Status as True and the DND option to Call Reject.

FeaturePriority overrides DND. It can have any of the following values:

- 1: No Priority
- 2: Urgent
- 3: Emergency

FeaturePriority in connect() API on CiscoCall represent a new capability. Pior releases already supported FeaturePriority in selectRoute() and redirect() API. When feature priority as EMERGENCY is specified in connect() API, and the destination terminal has DND–R enabled, the call still rings at the destination terminal and overrides the DND–R settings.

When a terminal has DND–R enabled and receives an intercom call, DND–R settings get overridden, and the call presents. This occurs because feature priority always remains 2 (URGENT) for intercom calls.

In non- shared line scenario where A calls B and Terminal B has DND–R enabled, CallCtlConnFailedEv with cause USER_BUSY gets delivered on A. The user sees the same behavior if DND–R is enabled on all the terminals that have shared DNs

In the case of shared lines when at least one terminal does not have DND–R enabled and a call is placed to the shared line, JTAPI delivers TermConnPassiveEv and CallCtlTermConnInUseEv for the terminals that have DND–R enabled (assuming the call was made with NORMAL feature priority). TermConnPassiveEv and CallCtlTermConnBridgedEv gets delivered if DND–R is disabled on the terminal during a call.

A new event CiscoTermDNDOptionChangedEv gets sent to the terminal observer whenever the DND option changes on the phone window or Common Phone Profile window in Cisco Unified Communications Manager Administration.

Note The default DND option specifies Ringer–off, and Route points do not support DND.

Backward Compatibility

Consider this feature as backward compatible.The application sees new events if this feature is configured. The new events can get filtered through TerminalEventFilter interface (CiscoTermEvFilter). By default, the filter stays disabled, and the new events do not get delivered.

Calling Party Normalization

Calling Party Normalization (CPN) enhancement includes the option to transform or normalize the incoming call number and convert it into the E.164 format, which includes the (country code, state code, and number type). The number type field identifies the subscriber as national, international, or unknown. The number type does not get supported in conference scenarios.

Backward Compatibility

Consider this feature as backward compatible.

Click to Conference

Click to Conference feature provides interfaces on SIP trunk for applications such as Instant Messenger (IM) to add parties to a conference. Users can add other parties to a conference or remove parties by using such applications. When Click to Conference is used to add a party to conference, a call gets offered to the target address. Only one connection for target address gets created on this initial call. This call then gets added to the conference, which results in a new callID for the call on the target address, and connections for other addresses in the call get created on the new call.

This section describes the interface changes that are done in Cisco JTAPI to handle the interactions when an address is added to a conference by using Click to Conference. When the Click to Conference feature is used, no consult call occurs, and JTAPI applications does not receive CiscoConferenceStartEv or CiscoConferenceEndEv.

Disable the feature by turning off the ENABLE CLICK TO CONFERENCE CallManager service parameter.

Backward Compatibility

Consider this feature as backward compatible. No change in JTAPI applications occurs when this feature is not configured or used.

Extension Mobility Username Login

The Extension Mobility Login Username enables applications to get the Extension Mobility login username from the Cisco Unified JTAPI controlled terminal.

Java Socket Connect Timeout

The Java Socket Connect Timeout enhancement enables the configuration of a timeout in seconds by using the Cisco Unified JTAPI specification and prevents connection delays to the primary CTIManager. The default specifies 15 seconds.

If the default of 15 seconds is unacceptable to the application, the default JAVA API of zero (0) sets the behavior to the normal JAVA Socket Connect API.

The range of values goes from 5 through 180 seconds. Zero defaults to Java behavior of the socket connect without any time out for connection.

Backward Compatibility

No backward compatibility impact exists.

selectRoute() with Calling Search Space and Feature Priority

The selectRoute() includes feature priority and calling search space parameters as an array. Ensure the same feature priority and calling search space are specified for all the routes that are selected. This API provides the flexibility of different feature priorities and calling search spaces for each route that is selected.

Backward Compatibility

No backward compatibility impact exists. The selectRoute() API remains functional and interoperates with the overloaded selectRoute() API.

Call Pickup

Call Pickup enhancement enables devices within a Call Pickup Group to be alerted that another phone in the group is ringing and to pick up the call—taking it from the original ringing device.

With this enhancement, support for observing terminals and addresses in which call pickup events exist, but JTAPI API still does not support invoking Call Pickup operations. This represents a small change in the way the API handles Call Pickup events when the service parameter "Auto Call Pickup" is enabled. If this parameter is disabled, when a user presses their "Pickup" softkey, their phone begins to ring, and they have all the normal actions available to them. If "Auto Call Pickup" is enabled, pressing the softkey immediately picks up the call without ringing.

Backward Compatibility

No backward compatibility impact exists.

Calling Party IP Address

This enhancement provides the calling party IP address to the destination side of basic calls, consultation calls for transfer and conference, and basic redirect/forwarding. Other scenarios and feature interactions do not get supported, including those instances during which the calling party changes.

Only IP phones as calling party devices get supported, although IP address of other calling devices may also get provided. New Cisco extensions to the CallCtlConnOfferedEv and RouteEvent classes get created and expose a method to obtain the calling party IP address. The new extensions comprise CiscoCallCtlConnOfferedEv and CiscoRouteEvent. An empty value returned indicates that calling party IP address info is not available.

Backward Compatibility Issues

Be aware that this release of JTAPI is backward compatible with applications that are written for Cisco Unified Communications Manager Administration Release 6.0, and CiscoJtapiClient upgrade is not mandatory.

Cisco Unified Communications Manager Administration Release 7.0 and JTAPI add Operating System Independence (OSI) support. This supports telephony features of Cisco Unified Communications Manager Administration Release 7.0 in both Linux and Windows 2003 server.

The Cisco Unified Communications Manager Administration features get ported from Cisco Unified Communications Manager Administration Release 6.0(x) (Appliance) to Cisco Unified Communications Manager Administration Release 7.0 (Win2003).

When a user upgrades from Cisco Unified Communications Manager Administration 4.x (Windows) to Cisco Unified Communications Manager Administration 7.0 (Windows/Linux), the plug-in URL to download the jtapi.jar differs. In Cisco Unified Communications Manager Administration Release 7.0, the plug-in URL from 6.x releases gets maintained.

The following URL applies for:

- Cisco Unified Communications Manager Administration Release 4.x (Windows): http://<servername or ip address>/CCMPluginsServer/jtapi.jar.
- Cisco Unified Communications Manager Administration Release 6.x and 7.0 (Linux): http://<server name or ip address>/plugins/jtapi.jar.
- Cisco Unified Communications Manager Administration Release 7.0 (Windows): http://<server name or ip address>/plugins/jtapi.jar.

The backward compatibility with regard to the plug-in URL does not get maintained between Cisco Unified Communications Manager Administration Release 4.x and Cisco Unified Communications Manager Administration Release 7.0.

Cisco Unified TAPI Developers Guide

The following sections describe the new and changed features and enhancements that were made to the *Cisco TAPI Developers Guide for Cisco Unified Communications Manager Release 7.0(1)*:

- Join Across Lines (SIP), page 125
- Localization Infrastructure Changes, page 126
- Do Not Disturb–Reject, page 126
- Calling Party Normalization, page 127
- Click to Conference, page 127
- Microsoft Windows Vista, page 127

For interface and message sequence changes, if any, refer to the *Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager Release 7.0(1)*.

Note Be aware that IPv6 is not supported.

Join Across Lines (SIP)

This feature allows two or more calls on different lines of the same device to get joined by using the join operation. Applications can use the existing join API to perform the task. When the Join Across Line feature happens, the consultation call on the different line on which the survival call does not reside will get cleared, and a CONFERENCED call that represents the consultation call will get created on the primary line where the conference parent is created. This feature should have no impact when you join multiple calls on the same line.

This feature gets supported on both SCCP and SIP devices that CTI controls. In addition, this feature also supports chaining of conference calls on different lines on the same device. Also, Join Across Line can occur on a non-controller (the original conference controller was on a different device than where the join is being performed) line.

This feature returns an error if one of the lines that are involved in the Join Across Lines is an intercom line.

Backwards Compatibility

Consider this feature as backward compatible.

Localization Infrastructure Changes

Beginning with Release 7.0, the systems automates TSP localization. The TSP UI can download the new and updated locale files directly from a configured TFTP sever location. As a result of the download functionality, Cisco TSP install supports only the English language during the installation.

During installation, the user inputs the TFTP server IP address. When the user opens the TSP UI for the first time, the TSP UI automatically downloads the locale files from the configured TFTP server and extracts those files to the resources directory. The languages tab in the TSP preferences UI also provides functionality to update the locale files.

Note To upgrade from Cisco Unified Communications Manager, Release 6.0(1) TSP to Cisco Unified Communications Manager, Release 7.0 TSP, ensure that Release 6.0(1) TSP was installed by using English. If Release 6.0(1) TSP is installed by using any language other than English and if the user upgrades to Release 7.0 TSP, the user must manually uninstall Release 6.0(1) TSP from Add/Remove programs in control panel and then perform a fresh install of Release 7.0 TSP.

Backward Compatibility

Only English locale gets packaged in Cisco TSP installer. The TSP UI downloads the locale files from the configured TFTP server, so the end user can select the required and supported locale after the installation.

Do Not Disturb–Reject

Do Not Disturb (DND) gets enhanced to support the rejection of a call. The enhancement Do Not Disturb–Reject (DND–R) enables the user to reject any calls when necessary. Prior to Cisco Unified Communications Manager Release 7.0, DND operated only with the Ringer Off option. If DND was set, the call would still get presented but without ringing the phone.

To enable DND–R, access the Cisco Unified Communications Manager Administration phone window, or the user can enable it on the phone. However, if the call has an emergency priority set, the incoming call getspresented on the phone even if the DND–R option is selected. This ensures that emergency calls do not get missed.

Also in a shared line scenario, if one of the lines is DND–R enabled and if the Remote In Use specifies True, call will get marked as connected inactive.

Backward Compatibility

Consider this feature as backward compatible.

Calling Party Normalization

Prior to Release 7.0, the "+" symbol did not display. Also, no support existed for displaying the localized or global number of the caller to the called party on its alerting display and the entry into its call directories for supporting a callback without the need of an Edit Dial.

This release adds support for "+" symbol. Also the calling number gets globalized and passed to the application. This allows the end user to dial back without using EditDial. Along with the globalized calling party, the user also gets the number type of the calling party. This helps the user to know where the call originated and whether it is a subscriber, national, or international number.

Backward Compatibility

Consider this feature as backward compatible.

Click to Conference

Click to Conference enables users to create conferences from an Instant Messaging (IM) application without creating a consult call first. The Cisco TSP treats the feature as an existing conference model. However, when the conference is created or dropped, the CtiExtendedReason may come as Click2Conference.

Backward Compatibility

Consider this feature as backward compatible.

Microsoft Windows Vista

The Cisco TSP client gets supported on Microsoft Windows Vista operating system with the following workarounds:

- Always perform the initial installation of the Cisco TSP and Cisco Unified Communications Manager TSP Wave Driver as a fresh install.
- If a secure connection to Cisco Unified Communications Manager is used, ensure the Windows Firewall is turned off/disabled.
- If Cisco Unified Communications Manager TSP Wave Driver is used for inbound audio streaming, ensure the Windows Firewall is turned off/disabled.
- If Cisco Unified Communications Manager TSP Wave Driver is used for audio streaming, ensure all other devices in the Sound, Video, and Game Controllers group are disabled.

Cisco Unified Communications Manager XML Developers Guide

The following sections describe the changes to *Cisco Unified Communications Manager XML Developers Guide, Release 7.0(1)*:

- Administrative XML Layer (AXL) Application Programming Interface, page 128
- AXL Serviceability Programming, page 131
- Cisco Web Dialer API, page 131

Administrative XML Layer (AXL) Application Programming Interface

The following sections provide information about updates to the AXL programming interface.

For More Information

Refer to *Cisco Unified Communications Manager XML Developers Guide* for detailed information about these updates.

Dynamic Throttling of Requests

Release 7.0 introduces a new throttling mechanism that takes into account the dynamic state of Cisco Unified Communications Manager. It considers the number of outstanding change notifications across the Cisco Unified Communications Manager cluster at any given time. Read requests never get throttled and pass through even when write requests are throttled.

AXL APIs

The following sections describe additions, modifications, and deprecations in the AXL APIs.

Added AXL APIs

The following list gives new AXL APIs in Release 7.0:

- addCalledPartyTransformationPattern
- removeCalledPartyTransformationPattern
- updateCalledPartyTransformationPattern
- getCalledPartyTransformationPattern
- addSIPTrunkSecurityProfile
- updateSIPTrunkSecurityProfile
- removeSIPTrunkSecurityProfile
- getSIPTrunkSecurityProfile
- addResourcePriorityNamespace
- updateResourcePriorityNamespace
- removeResourcePriorityNamespace
- getResourcePriorityNamespace
- addResourcePriorityNamespaceList
- updateResourcePriorityNamespaceList
- getResourcePriorityNamespaceList
- removeResourcePriorityNamespaceList
- addResourcePriorityDefaultNamespace
- updateResourcePriorityDefaultNamespace
- getResourcePriorityDefaultNamespace
- removeResourcePriorityDefaultNamespace
- addSIPProfile
- updateSIPProfile

- getSIPProfile
- removeSIPProfile
- addTODAccess
- updateTODAccess
- getTODAccess
- removeTODAccess
- getMobileSmartClientProfile
- addVG224
- updateVG224
- removeVG224
- getVG224
- addApplicationUser
- updateApplicationUser
- removeApplicationUser
- getApplicationUser

Modified AXL APIs

The following list gives AXL APIs that are modified in Release 7.0:

- addDevicePool
- updateDevicePool
- getDevicePool
- addMGCPEndPoint
- addSIPTrunk
- updateSIPTrunk
- getSIPTrunk
- addH323Phone
- updateH323Phone
- getH323Phone
- addH323Trunk
- updateH23Trunk
- getH323Trunk
- addH323Gateway
- updateH323Gateway
- getH323Gateway
- addRoutePattern
- updateRoutePattern
- getRoutePattern
- addHuntPilot

- updateHuntPilot
- getHuntPilot
- addTransPattern
- updateTransPattern
- getTransPattern
- addConferenceBridge
- updateConferenceBridge
- getConferenceBridge
- addCTIRoutePoint
- updateCTIRoutePoint
- getCTIRoutePoint
- addPhone
- updatePhone
- getPhone
- addGatewayEndpoint
- updateGatewayEndpoint
- getGatewayEndpoint
- addMOHServer
- updateMOHServer
- getMOHServer
- addVoiceMailPort
- getVoiceMailPort
- addCommonDeviceConfig
- updateCommonDeviceConfig
- getCommonDeviceConfig
- addTranscoder
- updateTranscoder
- getTranscoder
- addRemoteDestinationProfile
- updateRemoteDestinationProfile
- getRemoteDestinationProfile
- addTransformationPattern
- updateTransformationPattern
- getTransformationPattern
- addTimePeriod
- updateTimePeriod
- getTimePeriod
- addTimeSchedule

- updateTimeSchedule
- getTimeSchedule
- addRemoteDestination
- updateRemoteDestination
- getRemoteDestination
- addUser
- updateUser
- getUser
- addRouteList
- updateRouteList
- getRouteList

Deprecated Service Parameter

The following service parameter gets deprecated in Release 7.0:

- MaxAXLWritesPerMinute

AXL Serviceability Programming

With Release 7.0, when trace compression is enabled, trace files get compressed.

Cisco Web Dialer API

Release 7.0 adds the following SOAP API methods:

- getProfileDetailSoap
- getPrimaryLine

Cisco Unified Communications Manager SCCP Messaging Guide

The following sections describe the changes to *Cisco Unified Communications Manager SCCP Messaging Guide, Release 7.0(1)*:

- SCCP Messages Added or Modified, page 131
- SCCP Messages Deprecated, page 132

SCCP Messages Added or Modified

Release 7.0 adds or modifies the following SCCP messages:

- StationAccessoryInfoMessage
- StationButtonTemplateReqMessage
- StationCallHistoryInfoMessage
- StationMediaTransmissionFailureMessage
- StationOpenMultiMediaReceiveChannelAck

- StationOpenMultiMediaReceiveChannelMessage
- StationOpenReceiveChannelAckMessage
- StationOpenReceiveChannelMessage
- StationRegisterMessage
- StationRegisterTokenReq
- StationServerResMessage
- StationStartMediaTransmissionAckMessage
- StationStartMediaTransmissionMessage
- StationStartMultiMediaTransmissionAckMessage
- StationStartMultiMediaTransmissionMessage
- StationStartMulticastMediaReceptionMessage
- StationStartMulticastMediaTransmissionMessage
- StationStartToneMessage
- StationStopToneMessage
- StationUpdateCapabilitiesV3Message

SCCP Messages Deprecated

Release 7.0 deprecates the following SCCP messages:

- StationStartSessionTransmissionMessage
- StationStopSessionTransmissionMessage

For More Information

- *Cisco Unified Communications Manager SCCP Messaging Guide, Release 7.0(1)*

Cisco Unified IP Phones

This section provides the following information:

- Malicious Call ID—SIP Support, page 140
- Mobile Connect Enhancements, page 141
- Personal Address Book and Fast Dials Enhancements, page 142
- Programmable Line Keys—SIP Support, page 142
- Join Across Lines and Single Button Barge—SIP Support, page 143
- Secure Indication Tone, page 144
- Select for Non-Shared Lines—SIP Support, page 145

See Table 11 for a listing of features and supported phone models.

New Cisco Unified IP Phone Quick Start Guide for Administrative Assistants

You can find a new Cisco Unified IP Phone Quick Start Guide, which is specifically for administrative assistants, on Cisco.com at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/admin_qrc/7_0/aa_card.pdf

The four-panel guide helps administrative assistants to quickly understand basic phone features and answers common questions.

Cisco Unified IP Phone Expansion Module 7914—SIP Support

Cisco Unified Communications Manager 7.0 supports the use of the Cisco Unified IP Phone Expansion Module 7914 with the following phones that are running SIP:

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

Be aware that prior to this release, the expansion module was compatible only with phones that were running SCCP.

Limitations and Restrictions with SIP IP Phones

For IP phones running SIP firmware, the maximum number of keys is 36, regardless of whether a Cisco Unified IP Phone Expansion Module 7914, 7915, or 7916 is used. The 36 key number includes the keys on the base phone (see the following examples).

Cisco Unified IP Phone Expansion Module 7914 36-Key Example

- If you had a Cisco Unified IP Phone 7970, 7971, or 7975 (SIP) (8 keys on each IP phone) with two Cisco Unified IP Phone Expansion Modules 7914, you can have 8 + 14 + 14 = 36.
- If you had a Cisco Unified IP Phone 7961, 7962, or 7965 (SIP) (6 keys on each IP Phone) with two Cisco Unified IP Phone Expansion Modules 7914, you can have 6 + 14 + 14 = 34.

Caution Cisco recommends that, when the IP phone is using SIP firmware, only one Cisco Unified IP Phone Expansion Module 7915 or 7916 should be used because the majority of the keys on the second expansion module cannot be used.

Alternatively, you may configure the Cisco Unified IP Phone Expansion Module 7915 or 7916 as a 12-button key expansion module. This disables the shift/page keys, which allows two expansion modules, 12 keys each, to be used with a single IP phone.

Where to Find More Information

- *Cisco Unified IP Phone Expansion 7914 Phone Guide*
- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*

Cisco Unified IP Phone Expansion Modules 7915 and 7916

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

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

Where to Find More Information

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

Busy Lamp Field (BLF) Enhancements

Cisco Unified Communications Manager 7.0 introduces the following enhancements for the Busy Lamp Field (BLF) feature:

- New “BLF alerting” state—If configured, a new BLF line state, “BLF alerting,” notifies the monitoring phone user that the monitored line is in an Alerting state (ringing). An animated icon, LED appearance, and optional tone indicate BLF alerting.
- New BLF Pickup action—If BLF alerting is configured and a call is ringing on the monitored phone, the monitoring user can press the BLF pickup button to pick up the call.

These BLF enhancements get supported on the following phones that run SIP and SCCP:

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G

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

Where to Find More Information

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

Call Forward All Loop Breakout and Prevention

Cisco Unified Communications Manager 7.0 introduces enhancements for the following Call Forward All features:

- Call Forward All Loop Prevention—Prevents the end-user from configuring a Call Forward All destination on the phone that will create a Call Forward All loop or that will create a forward chain with more hops than the existing Forward Maximum Hop Count service parameter allows.
- Call Forward All Loop Breakout—Detects and breaks Call Forward All loops, which allows the call to ring on the phone that would have closed the loop. Prior to this release, the call got cleared if a Call Forward All loop was detected through the Forward Maximum Hop Count service parameter.

These Call Forward All features get supported on the following phones that are running SIP and SCCP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Calling Party Normalization and E.164

Cisco Unified Communications Manager 7.0 introduces support for the "+" symbol to represent international access codes for received numbers that is stored in call logs and directories.

If your phone system is configured for international call logging, the call logs, redial, or call directory entries may display a "+" symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the "+" may get replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the "+" with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes. Ask your phone administrator for more information regarding your phone system support for international call logging.

Note You can also use the international escape character in Fast Dials. If your phone system is configured for international call logging, users can enter the "+" symbol in the Cisco Unified CM User Options by choosing **User Options > Fast Dials**.

The following phones support this feature:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Wireless Phone 7921G (SCCP only)
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7985 (SCCP only)
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7975G

Extension Mobility Equivalency Enhancement

Cisco Unified Communications Manager 7.0 provides an enhancement to the Extension Mobility (EM) equivalency mechanism (also known as feature safe) to include additional models:

- Cisco Unified IP Phone models 7970G, 7971G-GE, and 7975G can share an EM profile.
- Cisco Unified IP Phone models 7961G, 7961G-GE, 7962G, and 7965G models can share an EM profile.
- Cisco Unified IP Phone models 7941G, 7941G-GE, 7942G, and 7945G models can share an EM profile.
- You can load an EM profile that is configured for a Cisco Unified IP Phone 7960G on to a 7961G, 7961G-GE, 7962G, or 7965G.
- You can load an EM profile that is configured for a Cisco Unified IP Phone 7940G on to a 7941G, 7941G-GE, 7942G, or 7945G.

Note This feature is not intended to support the use of an EM profile that is configured for a newer model back to the Cisco Unified IP Phone 7960G or 7940G.

Tip In addition to reviewing this section, see the "Cisco Extension Mobility Feature Safe Enhancements Require Cisco Unified Communications Manager 7.0 Device Package" section on page 18.

Table 10 provides a compatibility matrix of the Cisco Unified IP Phones that support this feature.

Table 10 Extension Mobility Equivalency Enhancement Feature Matrix

Cisco Unified IP Phone Model	7940	7941	7942	7945	7960	7961	7962	7965	7970	7971	7975
7940	N/A	Y	Y	Y	N	N	N	N	N	N	N
7941	N	N/A	Y	Y	N	N	N	N	N	N	N
7942	N	Y	N/A	Y	N	N	N	N	N	N	N
7945	N	Y	Y	N/A	N	N	N	N	N	N	N
7960	N	N	N	N	N/A	Y	Y	Y	N	N	N
7961	N	N	N	N	Y	N/A	Y	Y	N	N	N
7962	N	N	N	N	Y	Y	N/A	Y	N	N	N
7965	N	N	N	N	Y	Y	Y	N/A	N	N	N
7970	N	N	N	N	N	N	N	N	N/A	Y	Y
7971	N	N	N	N	N	N	N	N	Y	N/A	Y
7975	N	N	N	N	N	N	N	N	Y	Y	N/A

Where to Find More Information

- *Cisco Unified Communications Manager Features and Services Guide*

Directed Call Pickup

Cisco Unified Communications Manager 7.0 introduces a new call pickup feature, Directed Call Pickup that allows a user to pick up an alerting call from a specific DN by pressing the group pickup softkey followed by the DN where the call is ringing.

Call pickup features in prior releases did not allow the user to specify the DN.

Directed Call Pickup gets supported on the following phones that are running SIP or SCCP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Do Not Disturb Reject

Do Not Disturb (DND) allows a user to toggle a DND State on/off for a device by using a phone button or softkey. The phone button lights in amber when the feature is activated.

Note The line button does not apply to the Cisco Unified IP Phone 7906 and 7911.

DND contains two options: DND No Ring and DND Reject. DND No Ring allows a user to turn off only the ringer during an incoming call. DND Reject disables all audible and visual notifications of an incoming call during the ring-in state. The administrator or the user con configure these option by using Cisco Unified CM User Options.

DND Reject gets supported on the following phones that run SCCP or SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone Expansion Module 7914

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*

Enhanced Services Provisioning

The Enhanced Services Provisioning enhancement allows Cisco Unified Communications Manager administrators to offer a wider variety of phone services on Cisco Unified IP Phones. Administrators can configure these services as default features or allow phone users to subscribe or unsubscribe to the services by using Cisco Unified CM User Options.

The changes from the user point of view follow:

- Additional services to which users can subscribe, depending on the configuration, may exist.
- You can assign services to a variety of buttons.

Enhanced Services Provisioning gets supported on the following phones that run SCCP or SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7945G

- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G

Where to Find More Information

- Enhanced IP Phone Services, page 73
- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*

Cisco Unified IP Phone 7931G—SIP Support

Cisco Unified Communications Manager 7.0 introduces SIP support for the Cisco Unified IP Phone 7931G.

Where to Find More Information

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

Malicious Call ID—SIP Support

Cisco Unified Communications Manager 7.0 supports the Malicious Call ID (MCID) feature on the following phones that are running SIP:

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

Be aware that prior to this release, MCID was compatible only with phones that were running SCCP.

Where to Find More Information

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

Mobile Connect Enhancements

Cisco Unified Communications Manager 7.0 includes the following Cisco Unified Mobility features for Cisco Unified IP Phone users:

- Remote Destination Access—Users can turn on or off mobile connect access to all remote destinations from their desk phones.
- Time of Day Mobility—Users can determine whether a call should reach a remote destination based on the time of day and day of the week when the call is received. For example, a user may want to allow certain calls to ring the remote destination only during business hours and other calls to ring the remote destination only on the weekend.

  Users can configure Time of Day Mobility through Cisco Unified CM User Options. To set up Time of Day Mobility, the phone user performs these tasks:

  1. Create access lists.
  2. Create a remote destination that includes a ring schedule and one of the following instructions to apply to the ring schedule:

  – Always ring the destination.

  – Ring the destination only if the caller is in the selected access list.
- Do not ring the destination if the caller is in the selected access list.

Cisco Unified Communications Manager 7.0 supports the Mobile Connect feature on the following phones that are running SIP and SCCP:

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

Where to Find More Information

- *Cisco Unified Communications Manager Features and Services Guide*

Personal Address Book and Fast Dials Enhancements

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

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

Personal Address Book and Fast Dials get supported on the following phones that are running SIP and SCCP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone Expansion Module 7914
- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Programmable Line Keys—SIP Support

Cisco Unified Communications Manager 7.0 introduces support for assigning call-handling features (such as call forward, redial, hold) to programmable line keys on the following phones that are running SIP:

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

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

Where to Find More Information

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

Join Across Lines and Single Button Barge—SIP Support

Cisco Unified Communications Manager 7.0 supports the Join Across Lines feature on the following phones that are running SIP:

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

Be aware that prior to this release, Join Across Lines was compatible only with phones that were running SCCP.

Cisco Unified Communications Manager 7.0 supports the Single Button Barge feature on the following phones that are running SIP:

- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G

- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Be aware that prior to this release, Single Button Barge was compatible only with phones that were running SCCP.

Where to Find More Information

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

Secure Indication Tone

In Cisco Unified Communications Manager 7.0, Cisco Unified IP Phones support protected calling, which plays a security tone at the beginning of a call to indicate that the connection is secure (encrypted) on both ends, which provides integrity and privacy to the call. Be aware that some features, such as conference calling, shared lines, Cisco Extension Mobility, and join across lines are not available when protected calling is configured. Protected calls do not get authenticated.

The following information applies to protected calling:

- When a Cisco Unified IP phone displays the lock icon, this indicates that the phone is configured for secure (encrypted) calls, but this does not necessarily mean that the connected phone is also protected.
- When a Cisco Unified IP phone is configured for protected calling, a security tone plays at the beginning of the call to indicate that the call is protected on both ends of the connection.
- If the call is connected to a non-protected phone, then the security tone does not play.
- Protected calling gets supported for voice calls only. Video calls do not get supported.

Features Disabled When Protected Calling Is Configured

The following IP phone features automatically change when the protected call feature is enabled in Cisco Unified Communications Manager:

- Shared lines get disabled.
- Maximum calls and busy trigger get set to **1**.
- Cisco Extension Mobility gets disabled.
- Join across Lines gets set to **OFF.**

Cisco Unified Communications Manager 7.0 supports the secure indication tone feature on the following phones that are running SCCP or SIP:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7970G

- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7975G

Where to Find More Information

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

Select for Non-Shared Lines—SIP Support

Cisco Unified Communications Manager 7.0 introduces support for manual "Select" for non-shared lines on the following phones that are running SIP:

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

Where to Find More Information

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

Table 11 lists Cisco Unified IP Phones that support new Cisco Unified Communications Manager 7.0 features.

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Programmable Line Keys (SIP)	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE	Programmable Line Keys—SIP Support, page 142
Do Not Disturb (DND) Reject	SCCP and SIP: 7906G 7911G Expansion Module 7914 7931G 7941G 7941G-GE 7961G 7961G-GE 7942G 7962G 7945G 7965G 7970G 7971G 7975G	Do Not Disturb Reject, page 138
Cisco Unified IP Phone Expansion Modules 7915 and 7916	SCCP and SIP: 7962G, 7965G 7975G	Cisco Unified IP Phone Expansion Modules 7915 and 7916, page 134
Cisco Unified IP Phone Expansion Module 7914 (SIP)	SCCP and SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE SCCP only: 7960	Cisco Unified IP Phone Expansion Module 7914—SIP Support, page 133

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Busy Lamp Field (BLF) Enhancements	SCCP and SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G	Busy Lamp Field (BLF) Enhancements, page 134
Call Forward All Loop Breakout and Prevention	SCCP and SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Call Forward All Loop Breakout and Prevention, page 135
Calling Party Normalization and E.164	SCCP and SIP: 7906G 7911G 7931G 7941G 7941G-GE 7961G 7961G-GE 7970G 7971G 7942G 7945G 7962G 7965G 7975G SCCP only: Wireless 7921G 7985G	Calling Party Normalization and E.164, page 136

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Extension Mobility Equivalency Enhancement	• Cisco Unified IP Phone models 7970G, 7971G-GE, and 7975G can share an EM profile. • Cisco Unified IP Phone models 7961G, 7961G-GE, 7962G, and 7965G models can share an EM profile. • Cisco Unified IP Phone models 7941G, 7941G-GE, 7942G, and 7945G models can share an EM profile. • You can load an EM profile that is configured for a Cisco Unified IP Phone 7960G on to a 7961G, 7961G-GE, 7962G, or 7965G. • You can load an EM profile that is configured for a Cisco Unified IP Phone 7940G on to a 7941G, 7941G-GE, 7942G, or 7945G.	Extension Mobility Equivalency Enhancement, page 136
Directed Call Pickup	SCCP and SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Directed Call Pickup, page 138

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Enhanced Services Provisioning	SCCP and SIP: 7906G 7911G 7931G 7941G 7941G-GE 7961G 7961G-GE 7942G 7962G 7945G 7965G 7970G 7971G 7975G	Enhanced Services Provisioning, page 139
Cisco Unified IP Phone 7931G—SIP Support	7931G	Cisco Unified IP Phone 7931G—SIP Support, page 140
Malicious Call ID—SIP Support	7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Malicious Call ID—SIP Support, page 140
Mobile Connect Enhancements	SCCP and SIP: 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Mobile Connect Enhancements, page 141

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Personal Address Book and Fast Dials Enhancement	SCCP and SIP: 7906G 7911G 7931G 7941G 7941G-GE 7961G 7961G-GE 7942G 7962G 7945G 7965G 7970G 7971G 7975G Expansion Module 7914	Personal Address Book and Fast Dials Enhancements, page 142
Join Across Lines and Single Button Barge—SIP Support	7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G	Join Across Lines and Single Button Barge—SIP Support, page 143

Table 11 Cisco Unified IP Phone Support for Cisco Unified Communications Manager 7.0 Features

Cisco Unified Communications Manager 7.0 Feature	Cisco Unified IP Phone Support	For more information, see
Secure Indication Tone	SCCP and SIP: 7906G 7911G 7931G 7941G 7941G-GE 7961G 7961G-GE 7970G 7971G 7942G 7962G 7945G 7965G 7975G	Secure Indication Tone, page 144
Select for Non-Shared Lines—SIP Support	7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G	Select for Non-Shared Lines—SIP Support, page 145

Cisco Unified CM User Options

Starting with 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 152.

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 specifies 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 the Cisco Unified CM User Options. This required field specifies a default of True, which means that the User ID displays. The change takes effect the next time that the user logs in to Cisco Unified CM User Options.

Installation/Upgrade (Migration) Considerations

After you install or upgrade to Cisco Unified Communications Manager 7.0, you can configure this functionality.

If you configured this functionality in release 6.1(2), you do not need to configure the functionality again.

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

Multisite WAN Deployment with Distributed Call Processing

The Cisco Unified Communications Manager Business Edition multisite WAN deployment model with centralized call processing consists of a single call processing appliance that provides services for up to 20 sites (one central site and 19 remote sites), and this model uses the IP WAN to transport IP telephony traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites. A multisite Cisco Unified Communications Manager Business Edition deployment with centralized call processing has the following benefits:

- Single platform for call processing, Cisco Unified Mobility, and integrated messaging
- Single point of administration for both call processing and integrated messaging, providing single sign-on capabilities for administration users as well as end users
- A common infrastructure for a converged solution

For more information on this topic, refer to the *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 7.x*.

Unified CMBE Migration

Direct migration from Unified CMBE to standalone Unified CM is not currently supported. However, beginning with Unified CM 7.0, you have the option to repurpose the Cisco Media Convergence Server (MCS) 7828-H3 or MCS 7828-I3 as either a Unified CM publisher in a new cluster or a subscriber in an existing cluster. The MCS 7828 cannot, however, be reinstalled as a Cisco Unity Connection server.

When used with Cisco Unified CM, the MCS 7828-H3 and 7828-I3 platforms provide performance and scalability equivalent to the MCS 7825-H3 and 7825-I3. Although the MCS 7828 platforms have more memory and more disk space, the CPU and the disk speeds of the MCS 7825 platforms are equivalent, and the CPU and I/O Wait performance are the main factors for server equivalency.

Note The Cisco MCS 7828-H3 and 7828-I3 come with Unified CMBE and cannot be ordered without the Cisco Unified CMBE software package.

Caveats

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

Caveats describe unexpected behavior on a Cisco Unified Communications server. Severity 1 caveats represent the most serious caveats, severity 2 caveats represent less serious caveats, and severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Unified Communications Manager Release 7.0 by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

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

To access the Bug Toolkit, log on to http://tools.cisco.com/Support/BugToolKit.

UsingBug Toolkit

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

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

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

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser

- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 Acccess the Bug Toolkit, http://tools.cisco.com/Support/BugToolKit.

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

Step 3 If you are looking for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field, and click **Go**.

Tip Click **Help** on the Bug Toolkit page for information about how to search for bugs, create saved searches, create bug groups, and so on.

Open Caveats

Open Caveats for Cisco Unified Communications Manager Release 7.0(2) As of January 27, 2009 describes possible unexpected behaviors in Cisco Unified Communications Manager Release 7.0, which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in the "Open Caveats for Cisco Unified Communications Manager Release 7.0(2) As of January 27, 2009" section on page 155 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.

- 003.003(003.144) = Cisco CallManager Release 3.3(4)
- 005.000(000.123) = Cisco Unified CallManager Release 5.0(1)
- 005.000(001.008) = Cisco Unified CallManager Release 5.0(2)
- 005.001(002.201) = Cisco Unified CallManager Release 5.1(3)

Note Because defect status continually changes, be aware that the "Open Caveats for Cisco Unified Communications Manager Release 7.0(2) As of January 27, 2009" section on page 155 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "UsingBug Toolkit" section on page 153.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats for Cisco Unified Communications Manager Release 7.0(2) As of January 27, 2009

The following information comprises unexpected behavior (as of January 5, 2009) that you may encounter in this release of Cisco Unified Communications Manager

CLI

- CSCsv38268 CLI takes 3 to 5 seconds to start.

CMCTI

- CSCsu08818 CTI manager crashed during upgrade.
- CSCsj58001 Mismatch of Unmodified/Modified value on transfer via CPN.
- CSCsl75766 When the user pressed the QRT softkey on the phone, CTIManager crashed.
- CSCsr30432 Unified CM fails to send NOTIFY

Call Processing

- **Database**
  - CSCsv78166 Share line of SIP-SCCP or SIP-SIP does not work properly.
  - CSCsv69294 Unified CM nodes out-of-sync causes difference in DND publish states.
- **Media Control**
  - CSCsu09237 Call may drop when no xcoder for MOH supporting G711 only.
  - CSCsw28145 Cisco Unified CM negotiates 4CIF for CUVA client.
- **Mobility**
  - CSCsx01971 Mobile connect ignores Unified CM calling party transofrmation.
- **SCCP**
  - CSCsu71797 Phone that is running SCCP cannot dial a DN with 24 digits in personal directory.
  - CSCsw68359 Need tracing when codec locking occurs because of call recording.
- **SIP Appservices**
  - CSCsr46082 Unified CM does not send updated CI to Sametime.
- **System**
  - CSCsh36576 Signaling DSCP from Unified CM is incorrect for CS5, CS6, CS7, EF.

- **Unknown**
  - CSCsw64941 Configure rerouting calling search space fails.

CPI OS

- CSCsk70971 Publisher server NTP down if configured NTP down or unreliable.
- CSCsq34569 SIP trunk "Worst Case" high traffic volume loses all callers.
- CSCsv49493 Journal aborted error causes 7828-H3 server to do down.

Database

- CSCsw45761 Replication does not work after **clusterreset** gets run.
- CSCsj40566 ASCII character support differs from 4.x.
- CSCsw88022 Database should start and function when DNS is unavailable.

Serv-SOAP

- CSCsx09368 Cannot start CDROnDemand Service + Log Collection APIs.

User Interfaces

- CSCsx23525 Unable to update route list that contains multiple route groups.

Voice SIP Stack

- CSCsv62133 SIP stack does not resend ACK after receiving duplicate 200 OK.

Zathras

- CSCsu92664 Voice Mail Port Wizard Blank page

Documentation Updates

This section contains information on Cisco Unified CM 7.0 documentation omissions, errors, and updates for the following areas:

Troubleshooting

Cisco Unified Communications Operating System Administration

This section contains information on documentation omissions, errors, and updates for Cisco Unified Communications Operating System Administration, including the following ones:

Parallel Upgrades from Unified CM Releases 5.x and 6.x to Unified CM Release 7.0

When you upgrade a cluster running a supported version of Cisco Unified Communications Manager 5.x or 6.x to Cisco Unified Communications Manager 7.0, 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.

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

Chapter 2 of the *Cisco Unified Communications Operating System Administration Guide* does not contain the following information.

Cisco Unified 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*.

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

Characters Allowed in a Pre-Shared Key

Chapter 6 of the *Cisco Unified Communications Operating System Administration Guide* does not contain the following information.

Pre-shared IPSec keys can contain only alphanumeric characters and hyphens, not white spaces or any other characters. If you are migrating from a Windows-based version of Cisco Unified Communications Manager, you may need to change the name of your pre-shared IPSec keys, so they are compatible with current versions of Cisco Unified Communications Manager.

Cisco Unified Communications Manager Administration

This section contains information on documentation omissions, errors, and updates for Cisco Unified Communications Manager Administration. This section includes documentation updates for the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager Features and Services Guide*, and the *Cisco Unified Communications Manager System Guide*.

This section contains information on the following topics:

Cisco Unified Communications Manager Administration Guide

Cisco Unified Communications Manager System Guide

Cisco Unified Communications Manager Features and Services Guide

Administrator Can Set User Credential Policy to Expire Without Making a Global Policy Change

The Credential Settings and Fields section of the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly includes the following information:

> For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

And, again, regarding the Does Not Expire checkbox:

> You cannot uncheck this check box if the policy setting specifies Never Expires.

For releases above 6.1(3), this is not true. An administrator can set a user credential policy to expire without making a global policy change.

Description for Phone Personalization Is Incorrect in Documentation

The *Cisco Unified Communications Manager Bulk Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Administration Guide* contain incorrect information on phone personalization. If you plan to configure the Phone Personalization setting in Cisco Unified Communications Manager Administration, use the following information:

The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. You can enable phone personalization in the Enterprise Parameter Configuration window, the Phone Configuration window, the Common Phone Profile Configuration window, or the Phone Template window in Cisco Unified Communications Manager Administration.

Tip To enable phone personalization via the Phone Personalization enterprise parameter, which supports all phones that work with Phone Designer, choose **System > Enterprise Parameter** in Cisco Unified Communications Manager Administration, enter **1** in the Value Parameter field, and click **Save** in the Enterprise Parameter Configuration window.

If you configure phone personalization in the Phone Configuration window (Device > Phone), Common Phone Profile Configuration window (Device > Device Settings > Common Phone Profile), or the Phone Template window (Bulk Administration > Phones > Phone Template), choose one of the following options from the Phone Personalization drop-down list box:

- **Disabled**-The user cannot customize the Cisco Unified IP Phone by using Phone Designer.
- **Enabled**-The user can use Phone Designer to customize the phone.
- **Default**-The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window.

You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer release notes. To obtain the Phone Designer documentation, go to the following URL:

http://www.cisco.com/en/US/products/ps9829/tsd_products_support_series_home.html

Considerations for LDAP Port Configuration

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

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

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

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

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

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

- 3268—When SSL is not required.

3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Device Pool Chapter Contains Incomplete Description for Device Pool Name Field

The "Device Pool Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* does not contain the supported characters that you can enter in the Device Pool Name field. In this field, you can enter alphanumeric characters, period (.), hyphen (-), underscore (_), or a blank space. You can enter up to 50 characters.

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

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

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

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

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

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

Set to Default button; for example, the Phone URL Parameters in the Enterprise Parameters Configuration window do not display a suggested value, so clicking the Set to Default button does not change the parameter that you configured.

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

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

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

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

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

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

AAR Group Chapter Includes Incorrect Description for Dial Prefix Field

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

Incorrect Information

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

Correct Information

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

Hunt Pilot Chapter Needs Clarification of Maximum Hunt Timer Setting

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

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

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

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

In addition, Cisco Unified Communications Manager only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.

Annunciator Chapter Contains Incorrect Information on Description Field

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

Gateway Configuration Chapter Contains Incorrect Information on Domain Name Field

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

Default Device Profile Chapter Incorrectly Includes Expansion Module Settings

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

Note The "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide* erroneously states that you can configure the Module 1 and Module 2 drop-down list boxes in the Default Device Profile Configuration window.

Information Omitted for Reroute Incoming Request to new Trunk based on Setting

Instead of using the information for the Reroute Incoming Request to new Trunk based on setting in the "SIP Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*/online help, use the following information when you configure the Reroute Incoming Request to new Trunk based on setting in the SIP Profile Configuration window in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Cisco Unified Communications Manager accepts the call, Cisco Unified Communications Manager uses the configuration for this setting to determine whether the call should get rerouted to another trunk.

From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call gets rerouted:

- Never— the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. Cisco Unified Communications Manager, which identifies the trunk by using the source IP address of the incoming packet and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived.
- Contact Info Header—If the SIP trunk uses a SIP proxy, choose this option. Cisco Unified Communications Manager parses the contact header in the incoming request and uses the IP address or domain name and signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If no SIP trunk is identified, the call occurs on the trunk on which the call arrived.
- Call-Info Header with purpose=x-cisco-origIP—If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Cisco Unified Communications Manager parses the Call-Info header, looks for the parameter, purpose=x-cisco-origIP, and uses the IP address or domain name and the signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If the parameter does not exist in the header or no SIP trunk is identified, the call occurs on the SIP trunk on which the call arrived.

Tip This setting does not work for SIP trunks that are connected to a Cisco Unified Presence proxy server or SIP trunks that are connected to originating gateways in different Cisco Unified CM groups.

Do Not Begin Starting and Ending Directory Numbers with a Zero (0)

In Table 3 of the "Cisco Unified Communications Manager Configuration" chapter, under Auto-registration Information, the descriptions of Starting Directory Number and Ending Directory Number omit the information that neither number should begin with a zero (0).

Time-of-Day Routing Chapter Omits Information About Defined Time Periods

The "Time-of-Day Routing" chapter of the *Cisco Unified Communications Manager System Guide* omits the following information.

- If you define a time period with a specific date, on that specified date, that period overrides other periods that are defined on a weekly basis.

Example:

Consider the following example:

- A time period, afterofficehours, that is defined as 00:00 to 08:00 from Monday to Friday exists.
- A time period, newyearseve, that is defined as 14:00 to 17:00 on December 31st exists.

In this case, on December 31st, the afterofficehours period will not be considered because it gets overriden by the more specific newyearseve period.

Number of Digits Field Description is Incorrect

The Application Dial Rules Configuration Error Checking section of the Dial Rules Overview chapter of the *Cisco Unified Communications Manager System Guide* mis-states information about the Number of Digits field.

The correct information follows:

The Number of Digits field supports digits between 1 and 100, as well as the plus sign (+), the asterisk (*), and the number sign (#). Enter the number of digits of the dialed numbers to which you want to apply this application dial rule. You cannot allow this field to be blank for a dial rule.

Licensing Chapter Omits Information on Adjunct Licensing

The "Licensing" chapter in the *Cisco Unified Communications Manager System Guide* omits the fact that an error occurs when you configure an application, for example, Cisco IP Communicator, as the adjunct device, and the adjunct device requires more device license units (DLUs) than the primary device; for example, the Cisco Unified IP Phone 7906.

With adjunct licensing, fewer device license units (DLUs) get consumed for adjunct (secondary) devices, such as Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, when these applications get used with a Cisco Unified IP Phone 79xx, which serves as the primary device. For adjunct licensing to work, the adjunct device must consume fewer or the same number of DLUs as the primary device.

For example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7970, Cisco IP Communicator consumes only 1 DLU. Adjunct licensing works because the Cisco Unified IP Phone 7970 consumes 5 DLUs and Cisco IP Communicator consumes 3 DLUs.

In another example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7906, adjunct licensing fails because the Cisco Unified IP Phone 7906 consumes 2 DLUs and Cisco IP Communicator consumes 3 DLUs.

To ensure that Cisco Unified Communications Manager treats Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator as adjunct (secondary) devices, configure the Primary Phone setting in the Phone Configuration window for Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, as described in the "Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Cisco TFTP Chapter Omits Configuration Tip on Centralized TFTP

The "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the following information on configuring centralized TFTP:

For centralized TFTP configurations, ensure that the main TFTP server exists in the cluster that runs the highest version of Cisco Unified Communications Manager; for example, if you are using a centralized TFTP server between a compatible Cisco Unified CM 4.x cluster and a Cisco Unified Communications Manager 7.0 cluster, ensure that your main TFTP server exists in the Cisco Unified Communications Manager 7.0 cluster. If the main TFTP server exists in the cluster that runs the lower version of Cisco Unified Communications Manager, the phones use the locale files from the lower version of Cisco Unified Communications Manager, which can cause issues with the phone; for example, the phone displays Undefined or ??? for the Do Not Disturb feature instead of displaying that DND is active. These errors display on the phone because the locale files that are served to the phones from the main cluster do not include the localized phrases.

Directory Numbers Chapter Includes Incorrect Example for Shared Lines and Call Forward Busy Trigger

The "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide* includes incorrect example for shared lines and call forward busy trigger. Use the following information instead of the information in the guide:

Devices with shared-line appearance support the Call Forward Busy Trigger and the Maximum Number of Calls settings. You can configure Call Forward Busy Trigger per line appearance, but the configuration cannot exceed the maximum number call setting for that directory number.

The following example demonstrates how three Cisco Unified IP Phones with the same shared-line appearance, directory number 2000, use Call Forward Busy Trigger and Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

- Cisco Unified IP Phone 1—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 2—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 3—Configured a for maximum call value of 2 and busy trigger value of 2

When Cisco Unified IP Phone User 1 dials directory number 2000 for the first call, all three devices ring. The user for Cisco Unified IP Phone 3 picks up the call, and Cisco Unified IP Phones 1 and 2 go to remote in use. When the user for Cisco Unified IP Phone 3 puts the call on hold, user can retrieve the call from the Cisco Unified IP Phone 1 or Cisco Unified IP Phone 2. When User 2 dials directory number 2000 for the second call, only Cisco Unified IP Phone 3 rings.

Media Termination Point (MTP) and Transcoder Chapters Omit Information on Call Throttling

The "Media Termination Points" and "Transcoders" chapters in the *Cisco Unified Communications Manager System Guide* do not include information on the MTP and Transcoder Resource Throttling Percentage service parameter, which supports the Cisco CallManager service. This parameter, which defines a percentage of the configured number of MTP or transcoder resources, allows Cisco Unified Communications Manager to extend the call to an MTP/transcoder that offers the best chance of successfully connecting the call. When the number of active MTP or transcoder resources is equal to or greater than the percentage that is configured for this parameter, Cisco Unified Communications Manager throttles (stops sending) calls to this MTP/transcoder. Cisco Unified Communications Manager hunts through the MRGL one time to find a MTP/transcoder that uses matching codecs on both sides of the call, If Cisco Unified Communications Manager cannot find an available MTP/transcoder with matching codecs, Cisco Unified Communications Manager returns to the top of the MRGL to repeat the search, which then includes those MTPs/transcoders that are in a throttled state and that match a smaller subset of capabilities for the call. Cisco Unified Communications Manager extends the call to the MTP/transcoder that is the best match for the call when Cisco Unified Communications Manager determines that a resource may be available; the call fails when the MTP/transcoder cannot allocate a resource for the call. In some cases, Cisco Unified Communications Manager perceives that a resource on a hardware MTP/transcoder is available, but the actual port on the hardware is not available.

For example, if you enter 40 for the Call Count service parameter, which supports the Cisco IP Voice Media Streaming Application service, for a software MTP or transcoder (or for hardware resources, if the maximum sessions is configured at 40, for example), and you set the MTP and Transcoder Resource Throttling Percentage service parameter to 95 percent, Cisco Unified Communications Manager throttles calls to the MTP/transcoder when 38 resources are used on this MTP/transcoder (.95 x 40 = 38). When a new request for an MTP or transcoder arrives, Cisco Unified Communications Manager checks whether the number of resources has dropped to 38 or less, and if so, extends the call to the MTP/transcoder.

For the maximum, minimum, and default values for this service parameter, click the question mark help in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration.

System Guide Erroneously Includes Voice-Messaging Chapters

In the online help and in the whole-book PDF on www.cisco.com, disregard the following chapters in the *Cisco Unified Communications Manager System Guide for Cisco Unified Communications Manager Business Edition*:

- "Voice Mail Connectivity to Cisco Unified Communications Manager"
- "SMDI Voice Mail Integration"
- "Cisco Unity Messaging Integration"
- "Cisco DPA Integration"

Cisco Unified Communications Manager Business Edition supports Cisco Unity Connection. For information on configuring Cisco Unity Connection in Cisco Unified Communications Manager Administration, refer to the *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition.*

CTI and Cisco Unified Communications Manager Attendant Console Chapters Omit Information on CTI Monitored Lines

To calculate the number of CTI monitored lines in a system, use the following formula:

number of pilot point DNs + (number of clients open * number of directory numbers per phone) + (number of parked directory numbers * number of open clients) = CTI Monitored Lines

CTI Chapter Does Not Describe How Line/Device CSS Works for Redirected Calls

The "Computer Telephony Integration" chapter in the *Cisco Unified Communications Manager System Guide* does not describe how line/device calling search spaces work for calls that are redirected via a CTI application. When a CTI application requests to redirect a call by using the Redirect API, Cisco Unified Communications Manager uses the configuration for the line/device calling search space for the redirected party.

SIP Chapter Omits Information on SIP Port Throttling

The "Understanding Session Initiation Protocol" chapter in the *Cisco Unified Communications Manager System Guide* omits the following information on SIP UDP port throttling.

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

These throttle thresholds apply only to SIP UDP ports and do not affect SIP TCP or TLS ports.

Tip Be aware that the enterprise parameter Denial-of-Service Protection Flag must be set to True for these parameter values to take effect.

Table 12 describes the configurable threshold values:

Table 12 SIP UDP Port Throttling Thresholds

Service Parameter	Default Value	Range	Definition
SIP Station UDP Port Throttle Threshold	50	10-500	The SIP Station UDP Port Throttle Threshold parameter defines the maximum incoming packets per second that Cisco Unified Communications Manager can receive from a single (unique) IP address that is directed at the SIP station UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.
SIP Trunk UDP Port Throttle Threshold	200	10-500	The SIP Trunk UDP Port Throttle Threshold defines the maximum incoming packets per second that a SIP trunk can receive from a single (unique) IP address that is directed at the SIP trunk UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

Tip If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Cisco Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to these parameters to take effect.

SIP Chapter Contains Information on Licensing That Does Not Apply

Disregard the following tip that displays in the "Understanding Session Initiation Protocol" chapter in the *Cisco Unified Communications Manager System Guide* and in the online help. It does not apply to Cisco Unified Communications Manager 7.0.

"Third-party (non-Cisco) SIP trunks that you add to Cisco Unified Communications Manager Administration 7.0 require licensing. To track device license units for the SIP trunk, you must configure the Allocated License Units field in the Trunk Configuration window. For more information on how licensing works for the SIP trunk, see Licenses for Applications."

Trunk Chapter Omits Restrictions for H.323/H.225 Trunks

The "Understanding Cisco Unified Communications Manager Trunks Types" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the following restriction for H.323/H.225 trunks.

You cannot configure more than one H.323 trunk of any type (gatekeeper or non-gatekeeper-controlled) between the same clusters. Configuring more than one H.323 trunk can break inbound calls because Cisco Unified Communications Manager uses the received IP address to choose which trunk handles the

call. If you configure more than one H.323 trunk between the same clusters, Cisco Unified Communications Manager may choose the wrong trunk device when a call gets processed. To avoid this issue, Cisco Unified Communications Manager checks the following configuration:

- Whether the remote Cisco Unified Communications Manager IP address that is configured for the trunk is the same as another remote Cisco Unified Communications Manager IP address for a configured trunk.
- Whether a remote Cisco Unified Communications Manager hostname for a configured trunk is the same as another remote Cisco Unified Communications Manager hostname for a configured trunk.

If you configure one trunk with an IP address, and you configure another trunk with a hostname that resolves to the same IP address, Cisco Unified Communications Manager does not detect this configuration, which causes duplicate trunk configuration and problems with call processing.

Cisco Unified Communications Manager cannot detect the configuration of a gatekeeper-controlled trunk and a non-gatekeeper controlled trunk or the configuration of multiple gatekeeper-controlled trunks between the same Cisco Unified Communications Manager clusters. Additionally, Cisco Unified Communications Manager cannot detect the configuration of a gatekeeper-controlled H.323 trunk with the configuration of an H.323 gateway that is accessible from that same gatekeeper-controlled H.323 trunk. These configurations can cause problems for call processing, so carefully configure your trunks in Cisco Unified Communications Manager to avoid these issues.

Tip If your configuration contains duplicate entries, you can upgrade to Cisco Unified Communications Manager 7.0; however, after you upgrade, delete the duplicate entries to avoid issues with call processing.

Calling Party Normalization Chapter Omits Information on Colon and Cisco Unified Communications Manager Assistant

The "Calling Party Normalization" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not describe the support for the colon (:) in the incoming prefix fields. For information on this support, see the "Calling Party Normalization" section on page 44.

Tip The "Calling Party Normalization" chapter does not state that Cisco Unified Communications Manager Assistant supports globalized and localized calling party numbers. For more information on this topic, see the "Cisco Unified Communications Manager Assistant Chapters Omit Information on Calling Party Normalization" section on page 170.

Call Back Chapter Omits Fact That Cisco Unified IP Phones Support the Programmable Line Key (PLK)

The Call Back chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information:

Many Cisco Unified IP Phones support the Cisco Call Back feature by using the programmable line key (PLK). The following URL lists the phone documentation that is available for the various Cisco Unified IP Phones:

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

cBarge Chapter Omits Information on Shared Line Restriction for Conferences

The "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not contain the following cBarge restriction for shared lines and conferences:

If the number of shared-line users in the conference is equal to or greater than the configuration for the Maximum Number of Calls setting for the device from which you are attempting to barge, the phone displays the message, Error Past Limit.

Note The "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide* does not contain the previous information in the shared lines section.

Cisco Unified Communications Manager Assistant Chapters Omit Information on Calling Party Normalization

The Cisco Unified Communications Manager Assistant chapters in the *Cisco Unified Communications Manager Features and Services Guide* do not state that Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs.

For Cisco Unified Communications Manager Assistant to display localized and globalized calling party numbers, you must configure calling party normalization. The configuration checklists in the Cisco Unified Communications Manager Assistant chapters do not contain cross references to the calling party normalization information. For information on how to configure calling party normalization, refer to the "Calling Party Normalization" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Tip The "Calling Party Normalization" chapter does not state that Cisco Unified Communications Manager Assistant supports globalized and localized calling party numbers.

Directed Call Park Chapter Requires Update on Reverting Calls That Are Parked

The "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide* contains the following information on call reversion, which is incorrect:

Incorrect Information

Updating a directed call park number causes Cisco Unified Communications Manager to immediately revert any call that is parked on that number. This occurs because, when you update a directed call park number, Cisco Unified Communications Manager actually deletes the old information and then adds the new information. At the point that the old information is deleted, a parked call on that number cannot remain parked or be retrieved in the usual way and must be reverted.

If you configure Directed Call Park, use the following information instead of the incorrect information:

Correct Information

If you update a directed call park number, Cisco Unified Communications Manager reverts any call that is parked on that number only after the Call Park Reversion Timer expires.

Do Not Disturb Chapter Omits Information on DND Feature Priority

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

Intercom Chapter Omits How to Configure an Intercom Line or Speed-Dial Button

The "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide* omits the following steps that should be taken to successfully configure an intercom line or speed-dial button.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, click **Call Routing > Intercom**.

a. Create the intercom partition.

Note When you add a new intercom partition, Cisco Unified Communications Manager automatically adds a new intercom calling search space that contains only the new partition. You can modify the new intercom calling search space later.

b. Create the intercom directory number.

Note Be aware that intercom partition and calling search space cannot be mixed with partition and calling search space for regular lines.

Step 2 Click **Device > Device Settings > Phone Button Template** and add the intercom line to an existing phone button template or create new template.

Note Be aware that the intercom line cannot be configured as the primary line.

Step 3 Choose **Device > Phone** and assign an intercom directory number to the intercom line.

Step 4 Configure the intercom directory number and set up intercom speed dial, if desired.

Note You can configure the intercom line with a predefined destination (speed dial) to allow fast access.

Where to Find More Information

- The "Intercom chapter" in the *Cisco Unified Communications Manager Features and Services Guide Release 7.0(1)*
- The "Intercom Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide Release 7.0(1)*

- The “Intercom Calling Search Space Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide Release 7.0(1)*
- The “Intercom Partition Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide Release 7.0(1)*
- The “Phone Button Template Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide Release 7.0(1)*

Information About Changing Region Bandwidth Settings When Video Calls Are Made

The following informational reference will get added to the Cisco Unified Communications Manager Administration documentation:

Refer to the “Regions” subtopic under the “Administration Considerations” topic of the “IP Video Telephony” chapter of the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

The reference will get added to the following topics of the Cisco Unified Communications Manager Administration documentation:

- document: *Cisco Unified Communications Manager System Guide*
  chapter: Understanding Video Telephony
  topic: Bandwidth Management
- document: *Cisco Unified Communications Manager System Guide*
  chapter: Call Admission Control
  topic: Bandwidth Calculations
- document: *Cisco Unified Communications Manager Administration Guide*
  chapter: Location Configuration
  topic: list of restrictions at the beginning of the chapter
- document: *Cisco Unified Communications Manager Administration Guide*
  chapter: Region Configuration
  topic: list of limitations and restrictions at the beginning of the chapter

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone

Symptom

When a remote destination (mobile phone) is not a smart phone and a call to this mobile phone is anchored through Cisco Unified Communications Manager, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

Possible Cause

If the calling party receives busy/reorder/disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. Cisco Unified Communications Manager cannot recognize this circumstance because no disconnect signals came from the provider. To verify whether this is the case, let the calling party wait for 45 seconds, when service provider will time out and send disconnect signals, upon which Cisco Unified Communications Manager can provide a **Resume** softkey to resume the call.

Recommended Action

Perform the following actions:

- Add the following command to the gateway:

  voice call disc-pi-off

- For the Cisco CallManager service, set the Retain Media on Disconnect with PI for Active Call service parameter to False.

Cisco Unified Mobility Chapter Omits Information about the DN Mask Field

The "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not include the following information in the description of the DN Mask field that displays in the Access List Member Configuration window:

Note If you want to filter an incoming call from a calling number that begins with a leading +, you must include the leading + in the DN Mask field unless any supported wild card prefixes the directory number. For example, if an end user wants to block +14081239876, the user access list needs to include either +14081239876 or !14081239876 in the DN Mask field.

Cisco Unified Mobility Chapter Omits Information About the Destination Number Field for a Remote Destination

The "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide* provides an incomplete description of the Destination Number field that is found in the Remote Destination Configuration window. The following information completes the description:

If the administrator configures the Incoming Calling Party settings in the Cisco Unified Communications Manager gateway, trunk, or device pool to globalize the incoming calling party number, configure the Destination Number of the remote destination in the E.164 format.

Example: For a remote destination with US area code 408 and destination number 5552222, configure the Destination Number as +14085552222.

Additionally, if globalized destination numbers are in use, set the Matching Caller ID with Remote Destination service parameter to Complete Match.

Cisco Unified Mobility Chapter Omits Information About Configuring the Mobile Voice Access Media Resource

The "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide* omits the following information about configuring the mobile voice access media resource:

Be aware that this configuration is required for making calls with the Mobile Voice Access feature. After the gateway collects the required digits from the user to make a call, the call gets transferred to the DN that is configured in this window. This DN can represent an internal DN to Cisco Unified Communications Manager, and the end user does not need to know the DN. The administrator must configure a dial-peer, so the MVA service can transfer the call from the gateway to this DN. Ensure that this DN is be placed in a partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN, as configured in the Inbound Calling Search Space for Remote Destination service parameter in the Clusterwide Parameters (System - Mobility) pane.

Cisco Unified Mobility Chapter Contains Incorrect Information About Configuring an H.323 Gateway for System Remote Access by Using PRI

In the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*, the procedure for configuring an H.323 gateway for system remote access by using PRI contains minor errors. The following procedure contains the corrected steps.

Procedure

Step 1 Configure the T1/E1 controller for PRI from PSTN.

Sample configuration:

- controller T1 1/0
- framing esf
- linecode b8zs
- pri-group timeslots 1-24

Step 2 Configure the serial interface for the PRI (T1/E1).

Sample configuration:

- interface Serial 1/0:23
- ip address none
- logging event link-status none
- isdn switch-type primary 4ess
- isdn incoming-voice voice
- isdn bchan-number-order ascending
- no cdp enable

Step 3 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later:

- application service CCM
- http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12):

- call application voice Unified CCM
- http://<Unified CMPublisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not be use them.

Step 4 Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 58888 pots
- service CCM *(Mobile Connect VXML application)*
- incoming called-number 58888

- no digit-strip

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 100 pots
- application CCM *(Mobile Connect VXML application)*
- incoming called-number 58888 *(where* 58888 *represents the Mobile Voice Access number)*
- no digit-strip

Step 5 Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configuredin the "Mobile Voice Access Media Resource Configuration" section of the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Unified Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Cisco Unified Mobility Chapter Contains Incorrect Information About Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

In the “Cisco Unified Mobility” chapter in the *Cisco Unified Communications Manager Features and Services Guide*, the procedure for configuring an H.323 gateway for system remote access by using hairpinning contains minor errors. The following procedure contains the corrected steps.

Procedure

Step 1 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3 (13) and later:

- application service CCM
- http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12):

- call application voice Unified CCM
- http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should use not them.

Step 2 Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 1234567 voip
- service CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<*ip_address of call manager*>

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 1234567 voip
- application CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<*ip_address of call manager*>

Step 3 Add a dial-peer for transferring calls to the Mobile Voice Access DN that is configuredthat is configured in the "Mobile Voice Access Media Resource Configuration" section of the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

Note This specifies the Mobile Voice Access DN that is configured with the **Media Resources > Mobile Voice Access** menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Step 4 Configure hairpin.

- voice service voip
- allow-connections h323 to h323

Interaction between the Apply Application Dial Rules on SOAP Dial Request Service Parameter and Cisco Web Dialer.

The list of service parameters in the Setting Service Parameters for the Webdialer Servlet section of the Cisco Web Dialer chapter includes the service parameter called **Apply Application Dial Rules on SOAP Dial Request**. This parameter specifies whether Application Dial Rules must be applied for a SOAP dial request. Setting this parameter to True causes Webdialer to apply the dial rules before making a call.

Cisco Unified Communications Manager Security Guide

This section contains information on documentation omissions, errors, and updates for security.

SIP Digest Username Length Limited to 32 Characters

The Configuring Digest Authentication for the SIP Phone chapter of the *Cisco Unified Communications Manager Security Guide* does not contain the following information.

The length of the SIP digest username is not limited; however, when Unified CM challenges the identity of the SIP user agent, if the SIP realm username exceeds 32 characters, it will not be accepted. This length limitation is hard coded and cannot be modified.

Running an NMAP Scan

The *Cisco Unified Communications Manager Security Guide* does not describe how to run a Network Mapper (NMAP) scan program. You can run this program on any Windows or Linux platform to perform vulnerability scans. NMAP represents a free and open source utility for network exploration or security auditing.

Note NMAP DP scan can take up to 18 hours to complete

Syntax

nmap -n -vv -sU -p <*port_range*> <*ccm_ip_address*>

where:

-n: No DNS resolution. Tells NMAP to never do reverse DNS resolution on the active IP addresses that it finds. Because DNS can be slow even with the NMAP built-in parallel stub resolver, this option can slash scanning times.

-v: Increases the verbosity level, which causes NMAP to print more information about the scan in progress. The system shows open ports as they are found and provides completion time estimates when NMAP estimates that a scan will take more than a few minutes. Use this option twice or more for even greater verbosity.

-sU: Specifies a UDP port scan.

-p: Specifies which ports to scan and overrides the default. Be aware that individual port numbers are acceptable, as are ranges that are separated by a hyphen (for example 1-1023).

ccm_ip_address: IP address of Cisco Unified Communications Manager

Definition of Locally Significant Certificate

The definition of Locally Significant Certificate (LSC) in the *Cisco Unified Communications Manager Security Guide* is corrected. An LSC cannot be issued by a third-party certificate authority (CA). An LSC is a digital X.509v3 certificate that CAPF issues. It is installed on a phone or JTAPI/TAPI/CTI application.

Cisco Unified Real-Time Monitoring Tool

This section contains information on documentation ommissions, errors, and updates for the Cisco Unified Real-Time Monitoring Tool:

Cisco Unified Real-Time Monitoring Tool Administration Guide

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Real-Time Monitoring Tool Administration Guide*:

Updated Simultaneous Alert Configuration Procedure

The "Simultaneous Alert Configuration" procedure on page 111 updates and replaces the "Configuring a Global E-Mail List for Alert Notifications" procedure in the "Working with Alerts" chapter of the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Cisco Unified IP Phones

This section contains information on documentation omissions, errors, and updates for Cisco Unified IP Phone documentation.

Cisco Unified IP Phone Expansion Module 7914 Phone Guide

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified IP Phone Expansion Module 7914 Phone Guide, Release*:

Features of the Expansion Module 7914

In the Features of the Expansion Module 7914 section, the table states:

Someone else has a call on hold - flashing red light

It should say

Someone else has a call on hold - flashing green light

Cisco Unified Communications Manager Assistant

This section contains information on documentation omissions, errors, and updates for Cisco Unified Communications Manager Assistant.

Online Help Notes for Hebrew and Arabic

In the *Cisco Unified Communications Manager Assistant User Guide*, the chapter called "Introduction to Cisco Unified Communications Manager Assistant" does not contain the following information that Hebrew and Arabic users may need to know: Beginning in Cisco Unified Communications Manager Release 6.1, you can obtain PDF versions of the *Cisco Unified Communications Manager Assistant User Guide* in Hebrew and Arabic as online help on the client PC that is running Cisco Unified Communications Manager Assistant. This means that this client must have Adobe Reader installed.

Directory Search Correction

In the *Cisco Unified Communications Manager Assistant User Guide*, chapter "Getting Started," section "Using the Directory," the following sentence exists:

"To search for a coworker, enter any portion of the first and/or last name for the person in the search fields and click **Search**. The directory displays a list of all users that match your search string."

Replace the preceding information with the following information:

To search in the directory, enter the first letter of the first name or the first letter of the last name, followed by other letters in the first or last name (for whichever name you are entering), and click **Search**. The results that match the search string display.

The following wildcards do not get supported:

- *
- #
- +

Creating Filter Lists for a Manager

In the *Cisco Unified Communications Manager Assistant User Guide*, chapter "How to Configure Manager Features," section "How to Create Filter Lists for a Manager," the following information now applies:

- Be aware that the + character is allowed in inclusive/exclusive filter configurations for managers via the browser-based configuration window for managers or the PC assistant console application. The + character signifies an international directory number that an end user may see (as a globalized number) in either the Cisco Unified Communications Manager directory or on their Cisco Unified IP Phone (under **Call Details > History**).
- The + character gets evaluated on an incoming call. For an incoming call to a manager, Cisco Unified Communications Manager Assistant will evaluate both localized and globalized numbers while it performs filter pattern matching.

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.
